Université Mohamed V- Agdal
Faculté des Sciences
Département de Mathématiques
Avenue Ibn Batouta, B.P. 1014, Rabat, Maroc
Filières SM et SMI
Algèbre 4

# Structures Algébriques
# Exercices Corrigés

Azzouz Cherrabi ElMostafa Jabbouri

Année 2007-2008

# Table des matières

# Chapitre 1

# Arithmétique

**Exercice 1.1** *On se propose de montrer de deux façons différentes que* $\forall n \in \mathbb{N}^*$, $\exists s, t \in \mathbb{N}$ : $n = 2^s(2t+1)$.

*1) Première méthode : Utiliser une récurrence généralisée sur* $n$.

*2) Deuxième méthode : En considérant l'ensemble* $A = \{m \in \mathbb{N} : 2^m/n\}$, *montrer que* $A$ *possède un plus grand élément noté* $s$ *et que* $n = 2^s(2t+1)$.

**Solution**

*1) * Pour* $n = 1$, $n = 2^0(2.0+1)$.

** Supposons que cette propriété est vraie pour tout* $k < n$.

** Pour* $n$ *: on distingue les deux cas suivants :*

- *Si* $n$ *est impair, alors* $\exists t \in \mathbb{N} : n = 2t+1$ *d'où* $n = 2^0(2t+1)$.
- *Si* $n$ *est pair, alors* $\exists k \in \mathbb{N}^* : n = 2k$ *et puisque* $k < n$, *il résulte de l'hypothèse de récurrence que* $k = 2^{s'}(2t+1)$ *avec* $s', t \in \mathbb{N}$. *Ainsi* $n = 2^{s'+1}(2t+1)$.

*2) On a* $A = \{m \in \mathbb{N} : 2^m/n\} \subset \mathbb{N}$, $A \neq \emptyset$ *car* $0 \in A$ *et* $A$ *est majoré, car* $\forall m \in A$, $m \leq \log n/\log 2$. *D'où* $A$ *possède un plus grand élément qu'on note* $s$. *Alors,* $n = 2^s k$ *et puisque* $2^{s+1} \nmid n$, $k$ *est impair, i.e.,* $\exists t \in \mathbb{N} : k = 2t+1$ *donc* $n = 2^s(2t+1)$.

**Exercice 1.2**

*1) Montrer que si* $a \in \mathbb{N}$ *et* $p$ *est un nombre premier, alors* $p/a$ *ou* $p \wedge a = 1$.

*2) En déduire que si* $p$ *et* $q$ *sont deux entiers naturels premiers et distincts, alors* $p \wedge q = 1$.

*3) Montrer que tout entier* $n \geq 2$ *admet un diviseur premier (Ind : Considérer l'ensemble* $D = \{d \in \mathbb{N}/\ d \geq 2$ *et* $d/n\}$, *montrer que* $D$ *possède un plus petit élément* $p$ *et que* $p$ *est premier).*

*4) En déduire que l'ensemble des nombres premiers est infini. (Ind : on suppose que l'ensemble* $\mathcal{P}$ *des nombres premiers est fini, i.e.,* $\mathcal{P} = \{p_1, \ldots, p_n\}$, *avec* $p_i$ *les nombres premiers, considérer l'entier* $m = p_1 \ldots p_n + 1$ *et utiliser 3)).*

**Solution**

*1) Soit* $d = p \wedge a$. *Puisque* $d/p$ *et* $p$ *est premier,* $d = 1$ *ou* $d = p$. *Ainsi* $p \wedge a = 1$ *ou* $p/a$.

*2) D'après la question précédente,* $p \wedge q = 1$ *ou* $p/q$ *et puisque* $q$ *est premier et* $p \neq q$, $p \wedge q = 1$.

*3) Soient* $n \geq 2$ *et* $D = \{d \in \mathbb{N} : d \geq 2$ *et* $d/n\}$. *On a* $D \neq \emptyset$ $(n \in D)$ *et* $D \subset \mathbb{N}$, *d'où* $D$ *possède un plus petit élément qu'on note* $p$. *Alors* $p$ *est premier, sinon,* $\exists d \notin \{1, p\}$ *tel que* $d/p$ *et par suite* $d/n$, *ce qui contredit le fait que* $p$ *est le plus petit élément de* $D$.

*4) Supposons que* $\mathcal{P} = \{p_1, \ldots, p_n\}$ *est fini et considérons* $m = p_1 \ldots p_n + 1$. *On a* $m \geq 2$, *d'où, d'après 3),* $\exists p$ *premier :* $p/m$ *et puisque* $p = p_i$, *alors* $p/p_1 \ldots p_n$ *donc* $p/1 = m - p_1 \ldots p_n$, *ce qui est absurde.*

**Exercice 1.3** *Soient* $a, b \in \mathbb{N}$.

*1) Montrer que si* $a \wedge b = 1$, *alors* $a \wedge (a+b) = b \wedge (a+b) = 1$ *et* $ab \wedge (a+b) = 1$.

*2) En déduire que si* $a \wedge b = d$, *alors* $(a+b) \wedge (a \vee b) = d$.

**Solution**

*1) Si* $d/a$ *et* $d/a+b$, *alors* $d/(a+b) - a = b$ *et par suite* $d = 1$. *On utilise le même raisonnement pour vérifier que* $b \wedge (a+b) = 1$.

*On a aussi* $ab \wedge (a+b) = 1$. *En effet, supposons que* $ab \wedge (a+b) \neq 1$, $\exists p$ *premier tel que* $p/ab$ *et* $p/(a+b)$, *alors* ($p/a$ *et* $p/(a+b)$) *ou* ($p/b$ *et* $p/(a+b)$) *et donc* $a \wedge (a+b) \neq 1$ *ou* $b \wedge (a+b) \neq 1$.

*2) Posons* $a = da'$ *et* $b = db'$, *alors* $a' \wedge b' = 1$ *et donc* $(a+b) \wedge (a \vee b) = ((da'+db') \wedge (da' \vee db')) = (d(a'+b') \wedge d(a'b')) = d.((a'+b') \wedge (a'b'))$ *et puisque* $a' \wedge b' = 1$, *on a, d'après la question précédente,* $(a'+b') \wedge (a'b') = 1$, *d'où* $(a+b) \wedge (a \vee b) = d$.

**Exercice 1.4**

*1) Soit* $n \in \mathbb{N} - \{0, 1\}$. *Montrer que tous les entiers suivants ne sont pas des nombres premiers :* $n! + 2, n! + 3, \ldots, n! + n$.

*2) Donner* 100 *entiers consécutifs non premiers.*

**Solution**

*1) On remarque que* $2/n! + 2, 3/n! + 3, ...$*et* $n/n! + n$.

*2) On prend* $n = 101$ *et* $n_k = n! + k$ *avec* $2 \leq k \leq 101$. *D'après la question précédente, les 100 entiers* $n_k$ *sont des entiers non premiers.*

**Exercice 1.5** *Soit* $p \in \mathbb{N} - \{0, 1\}$. *Montrer que si* $(p-1)! \equiv -1 (\operatorname{mod} p)$, *alors* $p$ *est un nombre premier.*

**Solution** *Supposons que* $p$ *n'est pas premier, alors* $\exists d \in \{2, ..., p-1\} : d/p$. *Comme* $d \in \{2, ..., p-1\}$, $d/(p-1)!$, *i.e.,* $(p-1)! \equiv 0 \pmod d$. *Or, on a* $(p-1)! \equiv -1 \pmod d$ *car* $d/p$, *contradiction.*

**Exercice 1.6** *Soient* $n \in \mathbb{N} - \{0, 1\}$ *et* $p$ *un nombre premier. Si* $p/n$, *on appelle* $p$*-valuation de* $n$, *et on la note* $v_p(n)$, *l'exposant de la plus grande puissance de* $p$ *divisant* $n$. *i.e.,* $v_p(n) = \sup\{\alpha \in \mathbb{N}^* / \ p^\alpha/n\}$. *Si* $p \nmid n$, *on convient que* $v_p(n) = 0$.

*1) Déterminer* $v_2(104)$, $v_3(243)$ *et* $v_5(81)$.

*2) Montrer que si* $n, m \in \mathbb{N} - \{0, 1\}$, *alors* $v_p(nm) = v_p(n) + v_p(m)$.

*3) Montrer que* $v_2(1000!) = 994$.

**Solution**

*1) On a* $104 = 2^3.13$, *d'où* $v_2(104) = 3$. *De même,* $v_3(243) = 5$ *et* $v_5(81) = 0$.

*2) Posons* $v_p(n) = \alpha$ *et* $v_p(m) = \beta$, *alors* $p^{\alpha+\beta}/nm$ *et donc* $\alpha + \beta \leq v_p(nm)$. *On a aussi* $p^{\alpha+\beta+1} \nmid nm$, *sinon* $p^{\alpha+1}/n$ *ou* $p^{\beta+1}/m$, *alors* $v_p(nm) = v_p(n) + v_p(m)$.

*3)* $1000! = 1.(2.1).3.(2.2).....999.(2.500) = 2^{500}.500!.k$ *avec* $2 \nmid k$, *donc, en utilisant 2),* $v_2(1000!) = 500 + v_2(500!)$. *Aussi,* $v_2(500!) = 250 + v_2(250!)$, $v_2(250!) = 125 + v_2(125!)$, $v_2(125!) = 62 + v_2(62!)$, $v_2(62!) = 31 + v_2(31!)$, $v_2(31!) = 15 + v_2(15!)$, $v_2(15!) = 7 + v_2(7!)$, $v_2(7!) = 3 + v_2(3!) = 4$ *et ainsi* $v_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$.

**Exercice 1.7** *Montrer que :*

*1)* $11/2^{123}+3^{121}$

*2)* $7/3^{2n+1}+2^{n+2}$

**Solution**

*1) On a* $2^5 \equiv -1 \pmod{11}$*, d'où* $2^{10} \equiv 1 \pmod{11}$*. Aussi, on a* $3^5 \equiv 1 \pmod{11}$*, alors* $2^{123}+3^{121}=(2^{10})^{12}.2^3+(3^{10})^{12}.3 \equiv 2^3+3 \equiv 0 \pmod{11}$*.*

*2)* $3^{2n+1}+2^{n+2}=(3^2)^n.3+2^n.4 \equiv 2^n(3+4) \equiv 0 \pmod{7}$*.*

**Exercice 1.8**

*1) Soient* $a, b \in \mathbb{Z}^*$*. On suppose qu'il existe* $q, c \in \mathbb{Z}$ *tels que* $b = aq + c$*. Montrer que* $a \wedge b = a \wedge c$*.*

*2) Soit* $k \in \mathbb{N}$*. Montrer que* $(5k+3) \wedge (2k-1)$ *divise* $11$ *et que* $(5k+3) \wedge (2k-1) = 1$ *si, et seulement si,* $k+5$ *n'est pas congru à* $0$ *modulo* $11$ *(Ind : Appliquer deux fois la réduction issue de 1)).*

*3) Soient* $a = 327$ *et* $b = 823$*. Résoudre l'équation :* $ax + by = 36$*.*

**Solution**

*1) Posons* $d = a \wedge b$ *et* $d' = a \wedge c$*. On a* $d/aq$ *et* $d/b$ *d'où* $d/b - aq$ *donc* $d/c$*. Puisque* $d/c$ *et* $d/a$*, alors* $d/d'$*. De même, on vérifie que* $d'/d$ *et ainsi* $d = d'$*.*

*2) * On a* $5k+3 = 2(2k-1)+(k+5)$*. Posons* $b = 5k+3, a = 2k-1$ *et* $c = k+5$*. En utilisant 1), on a :* $(5k+3) \wedge (2k-1) = (2k-1) \wedge (k+5)$*. On a aussi* $2k-1 = 2(k+5)-11$*, alors* $(2k-1) \wedge (k+5) = (k+5) \wedge 11$ *et ainsi* $(5k+3) \wedge (2k-1) = (k+5) \wedge 11$ *divise* $11$*.*

** On a* $(k+5) \wedge 11 = 1$ *si, et seulement si,* $k+5 \not\equiv 0 \pmod{11}$*, car* $11$ *est premier, d'où* $(5k+3) \wedge (2k-1) = 1$ *si, et seulement si,* $k+5 \not\equiv 0 \pmod{11}$*.*

*3) On prend* $k = 164, a = 2k-1 = 327$ *et* $b = 5k+3 = 823$ *;* $k+5 = 169 \equiv 4 \pmod{11}$ *d'où, d'après 2),* $a \wedge b = 1$*.*

*On a* $(k+5) \wedge 11 = 1$*. Utilisons l'algorithme d'Euclide pour déterminer* $s, t \in \mathbb{Z}$ *tels que* $s(k+5)+11t = 1$ *;* $k+5 = 169 = 11 \times 15 + 4, q_1 = 15, r_1 = 4; 11 = 4 \times 2 + 3, q_2 = 2, r_2 = 3; 4 = 3 \times 1 + 1, q_3 = 1, r_3 = 1$*, alors* $1 = (1+q_2q_3)(k+5) + 11(-q_1 - q_3 - q_1q_2q_3) = 3(k+5) - 46.11$ *; on prend* $s = 3$ *et* $t = -46$*.*

*Utilisons la réduction 1) pour déterminer* $u, v \in \mathbb{Z}$ *tels que* $ub+va = 1$*. On a* $s(k+5)+11t = 1$*, alors* $1 = s(b-2a) + t[2(k+5) - a] = s(b-2a) + t[(2b-4a) - a] = (s+2t)b + (-2s-5t)a$ *et ainsi, on prend* $u = s+2t = -89$ *et* $v = -2s-5t = 224$*, d'où* $36ub + 36va = 36$*, alors* $(x-36v)a + (y-36u)b = 0$ *(*), ainsi* $b/(x-36v)a$ *et par suite* $b/(x-36v)$*, car* $a \wedge b = 1$*. Alors,* $x = 36v + mb$*, où* $m \in \mathbb{Z}$*. En remplaçant* $x$ *par* $36v + mb$ *dans (*), on obtient* $y = 36u - ma$*. On vérifie facilement que* $x = 36v + mb$ *et* $y = 36u - ma$ *est solution de l'équation et ainsi* $S = \{(36v + mb, 36u - ma)/m \in \mathbb{Z}\}$ $=\{(8064 + mb, -3204 - ma)/m \in \mathbb{Z}\}$*.*

**Exercice 1.9**

*1) Déterminer* $x_1, x_2 \in \mathbb{Z}$ *tels que* $\begin{cases} x_1 \equiv 1 \ (modulo\ 28) \\ x_1 \equiv 0 \ (modulo\ 19) \end{cases}$ *et* $\begin{cases} x_2 \equiv 0 \ (\ modulo\ 28) \\ x_2 \equiv 1 \ (modulo\ 19) \end{cases}$ .

*2) Déterminer* $x \in \mathbb{Z}$ *tel que* $\begin{cases} x \equiv 13 \ (modulo\ 28) \\ x \equiv 9 \ (modulo\ 19) \end{cases}$ .

**Solution**

*1) On a* $28 \wedge 19 = 1$, *d'où* $19.3 + (-2).28 = 1$. *En posant* $c_1 = 19u = 57$ *et* $c_2 = 28v = -56$, *on obtient* $\begin{cases} c_1 \equiv 1 \ (modulo\ 28) \\ c_1 \equiv 0 \ (modulo\ 19) \end{cases}$ *et ainsi* $x_1 \equiv c_1$ *(modulo* $28.19 = 532$*). De même,* $x_2 \equiv c_2$ *(modulo* $28.19 = 532$*).*

*2) Posons* $b_1 = 13$ *et* $b_2 = 9$ *alors* $\begin{cases} x \equiv 13 \ (modulo\ 28) \\ x \equiv 9 \ (modulo\ 19) \end{cases}$ *si, et seulement si,* $x \equiv b_1c_1 + b_2c_2$ *(modulo* $28.19 = 532$*), i.e,* $x \equiv 13.57 - 9.56 = 237$ *(modulo* $28.19 = 532$*).*

**Exercice 1.10**

*1) Soit* $p$ *un nombre premier.*

*a) Montrer que pour tout entier naturel non nul* $k < p$, *on a* $p|C_p^k$.

*b) En déduire le petit théorème de Fermat : si* $p$ *est premier, alors pour tout entier* $x$ *tel que* $x \not\equiv 0 \pmod p$, *on a* $x^{p-1} \equiv 1 \pmod p$.

*2) Soit* $n \in \mathbb{N}^*$. *On appelle* ***Indicateur d'Euler*** *de* $n$ *le nombre, noté* $\varphi(n)$, *des entiers* $m$ *tels que* $1 \leq m \leq n$ *et* $m \wedge n = 1$. *i.e.,* $\varphi(n) = card\{m \in \mathbb{N} : 1 \leq m \leq n \text{ et } m \wedge n = 1\}$.

*a) Calculer* $\varphi(6), \varphi(8), \varphi(13)$ *et* $\varphi(p)$ *si* $p$ *est premier.*

*b) Montrer que si* $p$ *et* $q$ *sont deux nombres premiers distincts, alors* $\varphi(pq) = (p-1)(q-1)$.*(Ind : Déterminer le nombre des* $m$ *tels que* $1 \leq m \leq pq$ *et* $m \wedge pq \neq 1$*).*

**Solution**

*1)*

*a) On a* $pC_{p-1}^{k-1} = kC_p^k$ *d'où* $p/kC_p^k$ *et puisque* $p \wedge k = 1$ *(*$k < p$ *et* $p$ *premier), alors* $p/C_p^k$.

*b) Utilisons maintenant une récurrence finie sur* $\{1, ..., p-1\}$ *pour montrer que* $x^p \equiv x \pmod p$. *Le résultat est évident pour* $x = 1$, *supposons que le résultat est vrai pour* $x$. *Alors,* $(x+1)^p = x^p + \sum_{k=1}^{p-1} C_p^k x^{p-k} + 1$. *Or, pour* $k : 1 \leq k \leq p-1$, $p|C_p^k$, *d'où* $(x+1)^p \equiv x^p + 1 \equiv x + 1 \pmod p$.

*Ainsi, pour tout entier* $x$, $p/x^p - x = x(x^{p-1} - 1)$, *comme* $p \wedge x = 1$, $p/(x^{p-1} - 1)$, *i.e.,* $x^{p-1} \equiv 1 \pmod p$.

*2)*

*a)* $\varphi(6) = 2$, $\varphi(8) = 4$, $\varphi(13) = 12$ *et puisque* $\forall k \in \{1, ..., p-1\}, k \wedge p = 1$, $\varphi(p) = p - 1$.

*b) Soit* $m$ *tel que* $1 \leq m \leq pq$. *On a* $m \wedge pq \neq 1$ *si, et seulement si,* $p/m$ *ou* $q/m$. *Alors, les entiers* $m$ *tels que* $1 \leq m \leq pq$ *et* $m \wedge pq \neq 1$ *sont exactement les multiples de* $p$ *ou de* $q$ *dans* $\{1, ..., pq\}$.

*Les multiples de* $p$ *dans* $\{1, ..., pq\}$ *sont* $p, 2p, ..., qp$ *et par suite, leur nombre est* $q$. *De même, le nombre des multiples de* $q$ *dans* $\{1, ..., pq\}$ *est* $p$. *Puisque* $pq$ *est le seul multiple commun de* $p$ *et* $q$ *dans* $\{1, ..., pq\}$, *le nombre des entiers* $m$ *tels que* $1 \leq m \leq pq$ *et* $m \wedge pq \neq 1$ *est* $p + q - 1$. *Ainsi, le nombre des entiers* $m$ *tels que* $1 \leq m \leq pq$ *et* $m \wedge pq = 1$ *est* $pq - (p + q - 1) = (p-1)(q-1)$ *et donc* $\varphi(pq) = (p-1)(q-1)$.

**Exercice 1.11 (Le cryptosystème RSA inventé par Rivest, Shamir et Adelman en 1977)**

*Une personne* ***A*** *veut utiliser le cryptosystème RSA, il prend deux nombres premiers* $p$ *et* $q$ *distincts, et pose* $n = pq$. *Il choisit un entier* $e$ *avec* $1 < e < \varphi(n)$ *et* $e \wedge \varphi(n) = 1$.

*1) Montrer qu'il existe un, et un seul, entier* $d$ *tel que :* $1 < d < \varphi(n)$ *et* $ed \equiv 1$ $(mod \varphi(n))$ *(utiliser l'identité de Bezout).*

*- Le couple* $(\mathbf{n}, \mathbf{e})$ *s'appelle* ***la clef publique de A*** *(cette clef est publiée sur Internet).*

*- Le couple* $(\mathbf{n}, \mathbf{d})$ *s'appelle* ***la clef privée de A*** *(p, q et d doivent rester secrets).*

*2) Montrer que pour tout entier x tel que* $1 < x < n$*, on a* $(x^e)^d \equiv x \pmod n$*. (Ind : montrer le résultat modulo p puis modulo q en utilisant l'exercice précédent).*

*3) Application : on prend* $p = 7, q = 17, e = 11$*,* $n = 119$ *et* $\varphi(n) = 96$*.*

*a) Trouver d tel que* $1 < d < 96$ *et* $ed \equiv 1 \pmod{96}$*.*

*b) On veut envoyer le message* $x = 5$ *à la personne A. Calculer* $y \equiv x^e \pmod n$ *(on chiffre le message x avec la clef publique de A).*

*c) A reçoit le message crypté y. Calculer* $y^d \pmod n$*, et montrer que A peut retrouver le message original x (A déchiffre le message codé y avec sa clef privée).*

**Solution**

*1) D'après le théorème de Bezout,* $\exists d_1, d_2 \in \mathbb{Z} : ed_1 + \varphi(n)d_2 = 1$*. Soit d le résidu de* $d_1$ *modulo* $\varphi(n)$*, d'où* $0 \leq d < \varphi(n)$ *et* $ed \equiv 1 \pmod{\varphi(n)}$*. Il est évident que* $d \notin \{0, 1\}$*. Supposons maintenant qu'il existe un entier* $d' : 1 < d' < \varphi(n)$ *et* $ed' \equiv 1$ $(mod \varphi(n))$*, alors* $\varphi(n)/e(d - d')$ *et par suite* $\varphi(n)/(d - d')$*, car* $e \wedge \varphi(n) = 1$*. Comme* $|d - d'| < \varphi(n)$*, on a* $d' = d$

*2) Puisque* $ed \equiv 1 \pmod{\varphi(n)}$*,* $\exists d' \in \mathbb{Z}$ *tel que* $ed + \varphi(n)d' = 1$*. Il est évident que* $d' \in \mathbb{Z}^-$ *et par suite posons* $d' = -d'' \in \mathbb{Z}^-$*. Distinguons les deux cas suivants :*

** Si* $x \wedge n = 1$*, on a* $x^{p-1} \not\equiv 0 \pmod q$*, sinon* $q/x$ *et par suite* $x \wedge n \neq 1$*. Alors, en utlisant le petit théorème de Fermat,* $(x^{p-1})^{q-1} \equiv 1 \pmod q$*. De même,* $(x^{q-1})^{p-1} = 1 \pmod p$*, d'où* $q/x^{\varphi(n)} - 1$ *et* $p/x^{\varphi(n)} - 1$*. Puisque p et q sont premiers et distincts, alors* $n = pq/x^{\varphi(n)} - 1$ *et ainsi* $x^{\varphi(n)} \equiv 1 \pmod n$*.*

*Comme* $ed - \varphi(n)d" = 1$*,* $(x^e)^d = x^1(x^{\varphi(n)})^{d"} \equiv x \pmod n$*, car* $x^{\varphi(n)} \equiv 1 \pmod n$*.*

** Si* $x \wedge n \neq 1$*, alors x est un multiple de p ou x est un multiple de q. Remarquons d'abord que x ne peut pas être un multiple commun de p et de q, sinon,* $n/x$ *ce qui est impossible car* $1 < x < n$*. Supposons que* $p/x$ *et que* $q \nmid x$ *(de même si* $q/x$ *et* $p \nmid x$*), alors* $x^{p-1} \not\equiv 0 \pmod q$ *d'où* $(x^{p-1})^{q-1} \equiv 1 \pmod q$*. Ainsi,* $(x^e)^d = x^1(x^{\varphi(n)})^{d"} \equiv x \pmod q$*, car* $x^{\varphi(n)} \equiv 1 \pmod q$ *et comme* $(x^e)^d \equiv x \equiv 0 \pmod p$*,* $(x^e)^d \equiv x \pmod n$*.*

*3)*

*a)* $e \wedge \varphi(n) = 1$*.* $\varphi(n) = 96 = 11.8 + 8$*,* $q_1 = 8, r_1 = 8$*,* $e = 11 = 8.1 + 3$*,* $q_2 = 1, r_2 = 3$*,* $r_1 = 8 = 3.2 + 2$*,* $q_3 = 2, r_3 = 2$*,* $r_2 = 3 = 2.1 + 1$*,* $q_4 = 1, r_4 = 1$*, alors* $r_4 = 1 = r_2 - r_3q_4 = r_2 - (r_1 - r_2q_3)q_4 = -r_1 + r_2(1 + q_3q_4) = -r_1 + (e - r_1q_2)(1 + q_3q_4) = e(1 + q_3q_4) - r_1(1 + q_2 + q_2q_3q_4) = e(1 + q_3q_4) - (\varphi(n) - eq_1)(1 + q_2 + q_2q_3q_4) = e(1 + q_1 + q_1q_2 + q_3q_4 + q_1q_2q_3q_4) + \varphi(n)(-1 - q_2 - q_2q_3q_4)$ *et par suite, on a* $d = 1 + q_1 + q_1q_2 + q_3q_4 + q_1q_2q_3q_4 = 35$*.*

*b) Calcul de* $5^{11}$ *(mod 119) : pour simplifier les calculs, on écrit l'exposant 11 en binaire :* $11 = (1011)_2$*, d'où* $5^{11} = 5^{2^3}.5^{2^1}.5^1 \equiv 67.25.5 \equiv 45 \pmod{119}$*.*

*c) Calcul de* $y^d = (45)^{35} \pmod n$*. on écrit l'exposant 35 en binaire :* $35 = (100011)_2$*, d'où* $y^d \equiv 45^{2^5}.45^2.45 \equiv 18.2.45 \equiv 5 \pmod{119}$*.*

*Lorsque A reçoit le message y, il calcule* $y^d \pmod n$ *et obtient x, car* $y^d = (x^e)^d \equiv x \pmod n$*.*

# Chapitre 2

# Groupes

**Exercice 2.1** *Soient $G$ un groupe, $H$ et $K$ deux sous-groupes de $G$ tels que $H \neq G$ et $K \neq G$. Montrer que $H \cup K \neq G$.*

**Solution**

*Si $H \subset K$ (resp. $K \subset H$), alors $H \cup K = K \neq G$ (resp. $H \cup K = H \neq G$). Supposons que $H \not\subseteq K$ et que $K \not\subseteq H$, alors $\exists h \in H : h \notin K$ et $\exists k \in K : k \notin H$. On a $hk \in G$, mais $hk \notin H \cup K$ car si $hk \in H$, alors $k = h^{-1}(hk) \in H$, de même si $hk \in K$.*

**Exercice 2.2 (Théorème de Wilson)** *Soit $p \in \mathbb{N}$. Montrer que si $p$ est un nombre premier, alors $(p-1)! \equiv -1 (\mathrm{mod}\, p)$. (Ind : considérer le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ et déterminer ses éléments $\bar{x}$ tels que $\bar{x} = \bar{x}^{-1}$).*

**Solution**

*On cherche d'abord les éléments $\bar{x} \in (\mathbb{Z}/p\mathbb{Z})^*$ tels que $\bar{x} = \bar{x}^{-1}$. On a $\bar{x} = \bar{x}^{-1}$ si, et seulement si, $\bar{x}^2 = \bar{1}$ si, et seulement si, $p/x^2 - 1 = (x-1)(x+1)$ si, et seulement si, $p/x - 1$ ou $p/x + 1$ ,i.e., $\bar{x} = \bar{1}$ ou $\bar{x} = \overline{-1} = \overline{p-1}$. Ainsi, si $\bar{k} \in \{\bar{2}, ..., \overline{p-2}\}$, i.e., $\bar{k} \in (\mathbb{Z}/p\mathbb{Z})^* - \{\bar{1}, \overline{p-1}\}$, alors $\bar{k}^{-1} \neq \bar{k}$ et $\bar{k}^{-1} \in \{\bar{2}, ..., \overline{p-2}\}$ d'où $\prod_{2 \leq k \leq p-2} \bar{k} = \bar{1}$ et ainsi $\overline{(p-1)!} = \bar{1}.\overline{p-1}. \prod_{2 \leq k \leq p-2} \bar{k} = \overline{p-1} = \overline{-1}\ (\mathrm{mod}\, p)$.*

**Exercice 2.3** *Soit $G =< a >$ un groupe cyclique d'ordre $n$.*

*1) Montrer que tout sous-groupe de $G$ est cyclique.*

*2) Soit $H \neq \{e\}$ un sous-groupe de $G$ et $m$ le plus petit entier strictement positif tel que $a^m \in H$. Montrer que $m/n$ et que $|H| = \frac{n}{m}$.*

*3) Montrer que si $d \in \mathbb{N}$ est tel que $d/n$, alors $G$ possède un unique sous-groupe d'ordre $d$.*

*Application : Déterminer le sous-groupe de $\mathbb{Z}/104\mathbb{Z}$ d'ordre 4.*

**Solution**

*1) Soit $H$ un sous-groupe de $G =< a >$. Supposons que $H \neq \{e\}$ (si $H = \{e\}$, $H =< e >$ est cyclique), alors, d'après le cours, $H =< a^m >$, avec $m$ est le plus petit entier strictement positif tel que $a^m \in H$.*

*2) On a $H =< a^m >$. En effectuant la division euclidienne de $n$ par $m$, on obtient $n = mq + r$ avec $(q, r) \in \mathbb{N} \times \mathbb{N}$ et $0 \leq r < m$.*

*Puisque* $G =< a >$ *est d'ordre* $n$, $e = a^n$ *d'où* $e = a^{mq}.a^r \in H$ *et comme* $a^{mq} = (a^m)^q \in H$ *car* $a^m \in H$, $a^r = (a^{mq})^{-1} \in H$. *Etant donné que* $m$ *est le plus petit entier strictement positif tel que* $a^m \in H$ *et que* $0 \leq r < m$, *alors* $r = 0$ *et ainsi* $m/n$.

*Posons* $|H| = o(a^m) = s$. *On a* $a^{ms} = (a^m)^s = e$ *d'où* $n/ms$ *et puisque* $m/n$, $\frac{n}{m}/s$. *D'autre part,* $(a^m)^{\frac{n}{m}} = a^n = e$ *d'où* $s/\frac{n}{m}$. *Alors* $s = \frac{n}{m}$.

*3) Si* $d = 1$, *alors* $H = \{e\}$ *est l'unique sous-groupe de* $G$ *d'ordre 1.*

*Supposons que* $d > 1$. *Soit* $H =< a^{\frac{n}{d}} >$. *Puisque* $d/n$, $\frac{n}{d}$ *est le plus petit entier strictement positif tel que* $a^{\frac{n}{d}} \in H$ *; en effet, si* $a^s \in H =< a^{\frac{n}{d}} >$, $a^s = (a^{\frac{n}{d}})^t$ *d'où* $a^{sd} = e$ *ainsi* $n/sd$ *et puisque* $d/n$, $\frac{n}{d}/s$. *Alors, d'après b),* $|H| = \frac{n}{\frac{n}{d}} = d$.

*De plus, Si* $K$ *est un sous-groupe de* $G$ *(d'ordre* $d$*) alors* $K =< a^m >$ *avec* $m$ *est le plus petit entier strictement positif tel que* $a^m \in K$ *et, d'après b), on a* $d = \frac{n}{m}$ *d'où* $K =< a^m >=< a^{\frac{n}{d}} >= H$.

*Application* : $\mathbb{Z}/104\mathbb{Z}$ *est un groupe cyclique et* $4/104$. *Alors,d'après c),* $\mathbb{Z}/104\mathbb{Z}$ *possède un unique sous-groupe* $H$ *d'ordre* $4$ *et* $H =< \frac{104}{4}.\bar{1} >=< \overline{26} >= \{\bar{0}, \overline{26}, \overline{52}, \overline{78}\}$.

**Exercice 2.4**

*1) Soit* $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$. *Montrer que* $\mathbb{Z}/n\mathbb{Z} =< \bar{m} >$ *si, et seulement si,* $m \wedge n = 1$.

*2) En déduire que si* $G$ *est un groupe cyclique d'ordre* $n$, *alors* $\varphi(n)$ *est le nombre des générateurs distincts de* $G$.

*3) Montrer que si* $d/n$, *alors* $\varphi(d)$ *est le nombre d'éléments de* $\mathbb{Z}/n\mathbb{Z}$ *d'ordre* $d$. *(ind. appliquer 2) à l'unique sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$ *d'ordre* $d$*).*

*4) En déduire que* $n = \sum_{d/n} \varphi(d)$.

**Solution**

*1) Supposons que* $\mathbb{Z}/n\mathbb{Z} =< \bar{m} >$, *alors* $\exists u \in \mathbb{Z} : \bar{1} = u\bar{m} = \overline{um}$, *i.e.,* $\exists v \in \mathbb{Z} : um + vn = 1$ *d'où* $m \wedge n = 1$. *Réciproquement, si* $m \wedge n = 1$, *alors* $\exists u, v \in \mathbb{Z} : um + vn = 1$ *d'où* $\overline{um} = \bar{1}$ $(\operatorname{mod} n)$ *et ainsi* $\mathbb{Z}/n\mathbb{Z} =< \bar{m} >$ *(si* $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ *alors* $\bar{x} = xu.\bar{m} \in < \bar{m} >$*).*

*2) Puisque* $G$ *est cyclique d'ordre* $n$, *alors* $G \simeq \mathbb{Z}/n\mathbb{Z}$. *Ainsi, d'après la question précédente, le nombre de générateurs de* $\mathbb{Z}/n\mathbb{Z}$ *n'est autre que le nombre des* $m : 1 \leq m \leq n$ *et* $m \wedge n = 1$.

*3) Soient* $H$ *l'unique sous-groupe de* $\mathbb{Z}/n\mathbb{Z}$ *d'ordre* $d$ *et* $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$. *On a* $o(\bar{m}) = d$ *si, et seulement si,* $H =< \bar{m} >$. *Ainsi le nombre des éléments de* $\mathbb{Z}/n\mathbb{Z}$ *d'ordre* $d$ *est égal au nombre des générateurs de* $H$.

*Comme* $H$ *est cyclique d'ordre* $d$, $H \simeq \mathbb{Z}/d\mathbb{Z}$. *Alors, d'après la question précédente, le nombre des générateurs de* $H$ *est* $\varphi(d)$.

*4) Soient* $d \in \mathbb{N}$ *et* $E_d = \{\bar{m} \in \mathbb{Z}/n\mathbb{Z} \ / \ o(\bar{m}) = d\}$. *Si* $d \nmid n$, *alors* $E_d = \emptyset$ $(o(\bar{m})/n, \forall \bar{m} \in \mathbb{Z}/n\mathbb{Z})$ *et si* $d/n$, *alors* $E_d = \{\bar{m} \in \mathbb{Z}/n\mathbb{Z} \ / \ o(\bar{m}) = d\} \neq \emptyset$ *(question 3) de l'exercice précédent). Aussi, si* $d \neq d'$, *alors* $E_d \cap E_{d'} = \emptyset$ *et* $\forall \bar{m} \in \mathbb{Z}/n\mathbb{Z}, \exists! d : \bar{m} \in E_d$. *Ainsi,* $(E_d)_{d/n}$ *forment une partition de* $\mathbb{Z}/n\mathbb{Z}$ *et par suite* $n = |\mathbb{Z}/n\mathbb{Z}| = \sum_{d/n} card(E_d)$. *Or, d'après 3),* $card(E_d) = \varphi(d)$ *et donc* $n = \sum_{d/n} \varphi(d)$.

**Exercice 2.5** *Soient* $G$ *un groupe fini,* $H$ *et* $K$ *deux sous-groupes de* $G$. *On pose* $L = H \cap K$ *et* $(K/L)_g = \{k_1L, \ldots, k_nL\}$, *où* $k_1L, ..., k_nL$ *sont les différentes classes de* $K$ *modulo* $L$ *à gauche.*

*1) Montrer que $k_1H, \ldots, k_nH$ forment une partition de $KH$.*
*2) En déduire que $card(KH) = \frac{|K|.|H|}{|H \cap K|}$.*

**Solution**
*1) On a :*
* $\forall i = 1, ..., n : k_iH \neq \emptyset$ *car* $k_i = k_ie \in k_iH$.
* *Si* $i \neq j$, $k_iH \cap k_jH = \emptyset$, *sinon* $\exists h, h' \in H : k_ih = k_jh'$ *alors* $k_j^{-1}k_i = h'h^{-1} \in H \cap K = L$ *d'où* $k_jL = k_iL$, *ce qui contredit le fait que* $k_jL \cap k_iL = \emptyset$.
* *On a* $\bigcup_{i=1}^{n} k_iH \subset KH$. *Vérifions alors l'autre inclusion : soit* $kh \in KH$. *Comme* $K = \bigcup_{i=1}^{n} k_iL$, *alors* $\exists j : k \in k_jL$ *d'où* $k = k_jl$, *avec* $l \in L$, *ainsi* $kh = k_j(lh) \in k_jH$ *car* $l \in L \subset H$ *et* $h \in H$.
*2) Puisque* $k_1H, \ldots, k_nH$ *forment une partition de* $KH$, $card(KH) = \sum_{i=1}^{n} card(k_iH)$. *En remarquant que* $\forall i = 1, ..., n$, $f : H \longrightarrow k_iH$, $h \longmapsto k_ih$ *est une bijection, on a* $card(k_iH) = |H|$ *d'où* $card(KH) = n|H|$. *D'après le théorème de Lagrange, on a* $n = [K : L] = \frac{|K|}{|L|}$ *d'où* $card(KH) = \frac{|K||H|}{|L|}$.

**Exercice 2.6** *Soient $G$ un groupe, $H$ et $K$ deux sous-groupes distingués de $G$ et tels que $H \cap K = \{e\}$.*
*1) Montrer que $\forall h \in H, \forall k \in K, hk = kh$.*
*2) Montrer que $HK$ est un sous-groupe distingué de $G$ et que $HK \simeq H \times K$.*

**Solution**
*1) On a* $\forall h \in H, \forall k \in K$, $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} \in K$ *car* $K \lhd G$ *et par suite* $hkh^{-1} \in K$. *De même,* $hkh^{-1}k^{-1} = h(kh^{-1}k^{-1}) \in H$. *D'où* $hkh^{-1}k^{-1} = H \cap K = \{e\}$ *et donc* $hk = kh$.
*2) Puisque* $HK = KH$, $HK$ *est un sous-groupe de* $G$. *On a aussi* $HK \lhd G$. *En effet, soit* $g \in G, h \in H, k \in K$, *alors* $ghkg^{-1} = (ghg^{-1})(gkg^{-1}) \in HK$ *car* $H$ *et* $K$ *sont distingués dans* $G$.
*Montrons que* $HK \simeq H \times K$. *Soit* $f : H \times K \longrightarrow HK, (h, k) \longmapsto hk$. $f$ *est évidemment une application surjective et en utilisant* $hk = kh, \forall h \in H, \forall k \in K$, *on vérifie facilement que* $f$ *est un homomorphisme de groupes.* $f$ *est aussi injectif. En effet, soit* $(h, k) \in \ker f$ *d'où* $hk = e$ *alors* $h = k^{-1} \in H \cap K = \{e\}$, *i.e.,* $h = k = e$.

**Exercice 2.7** *Soit $G$ un groupe.*
*1) Montrer que si $|G|$ est pair, alors $G$ possède un élément d'ordre 2. (Considérer l'ensemble $E = \{x \in G / x \neq x^{-1}\}$).*
*2) Soit $G$ un groupe non cyclique d'ordre 6 et $a$ un élément de $G$ d'ordre 2.*
*a) Montrer que si $b \in G : o(b) = 2$ et $ab = ba$, alors $b = a$. (Ind : considérer le sous-groupe $< a, b >$).*
*b) Montrer que $G$ possède un élément d'ordre 3. (Ind. soit $b \in G - \{a, b\}$. Montrer que si $o(b) = 2$ alors $o(ab) = 3$).*
*c) Dans la suite, on note $c$ cet élément.*
*i) Montrer que $ac \neq ca$ et que $G = \{e, a, c, c^2, ac, ac^2\}$.*
*ii) En déduire que $ca = ac^2$ et que $G \simeq S_3$. (Ind. considérer la table de multiplication de $G$).*

**Solution**

*1) Soit $E = \{x \in G / x \neq x^{-1}\}$. Supposons que $E \neq \emptyset$, sinon $\forall x \in G : x^2 = e$ et puisque $|G| > 1$, il suffit de prendre $x \neq e$. On remarque que si $x \in E$, alors $x^{-1} \in E$ et $x \neq x^{-1}$ d'où $card(E)$ est pair et par suite $card(G - E)$ est pair. Comme $e \in (G - E)$, $\exists x \in G - E : x \neq e$ et ainsi $o(x) = 2$.*

*2) a est un élément de G d'ordre 2 (un tel élément existe car $|G| = 6$ est pair (question 1)).*

*a) Si $b \neq a$ alors $H = \{e, a, b, ab\}$ est un sous-groupe de G, ce qui est faux car $|H| = 4 \nmid |G| = 6$.*

*b) Soit $b \in G - \{e, a\}$. Puisque G est non cyclique et $b \neq e$, $o(b) \in \{2, 3\}$. Supposons que $o(b) = 2$ alors $o(ab) \in \{1, 2, 3, 6\}$. Or, $o(ab) \neq 1$ sinon $b = a$, $o(ab) \neq 2$ sinon $ab = ba$ et par suite $b = a$ (utiliser a)) et $o(ab) \neq 6$ sinon $G =< ab >$ est cyclique. Alors $o(ab) = 3$.*

*c)*

*i) Si $ac = ca$, alors $o(ac) = 6$. En effet, $o(ac) \neq 1$ sinon $ac = e$ et donc $c = a$, $o(ac) \neq 2$ sinon $(ac)^2 = a^2c^2 = c^2 = e$ et $o(ac) \neq 3$ sinon $(ac)^3 = a^3c^3 = a = e$ et donc $o(ac) = 6$. D'où G est cyclique, contradiction.*

*Puisque $o(a) = 2 \nmid | < c > | = 3$, $a \notin < c >$ d'où $e, c, c^2, a$ sont des éléments de G deux à deux distincts. On vérifie facilement que $e, c, c^2, a, ac, ac^2$ sont des éléments de G deux à deux distincts et donc $G = \{e, c, c^2, a, ac, ac^2\}$.*

*ii) On a $ca \neq e$, sinon $c = e$, $ca \neq c$, sinon $a = e$, $ca \neq c^2$, sinon $a = c$, $ca \neq a$, sinon $c = e$. On a aussi, d'après la question précédebte, $ca \neq ac$ d'où $ca = ac^2$.*

*(On peut aussi remarquer que $[G :< c >] = 2$ alors, d'après le cours, $< c > \lhd G$ et par suite $aca^{-1} \in < c >$. $aca^{-1} \neq e$ car $c \neq e$ et $aca^{-1} \neq c$ car $ac \neq ca$, alors $aca^{-1} = c^2$ et ainsi $ca = ac^2$).*

*La table de multiplication de G est*

| ↱ · | $e$ | $a$ | $ac$ | $ac^2$ | $c$ | $c^2$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $ac$ | $ac^2$ | $c$ | $c^2$ |
| $a$ | $a$ | $e$ | $c$ | $c^2$ | $ac$ | $ac^2$ |
| $ac$ | $ac$ | $c^2$ | $e$ | $c$ | $ac^2$ | $a$ |
| $ac^2$ | $ac^2$ | $c$ | $c^2$ | $e$ | $a$ | $ac$ |
| $c$ | $c$ | $ac^2$ | $a$ | $ac$ | $c^2$ | $e$ |
| $c^2$ | $c^2$ | $ac$ | $ac^2$ | $a$ | $e$ | $c$ |

*. (Pour ne pas effectuer tous les calculs, on utilise le fait que cette table est un carré latin).*

*L'homomorphisme $f : G \longrightarrow S_3$ défini par $f(a) = (12)$, $f(c) = (123)$ est un isomorphisme de groupes.*

**Exercice 2.8** *Soit $Gl_2(\mathbb{C})$ le groupe des matrices carrées d'ordre 2 inversibles à coefficients dans $\mathbb{C}$. On considère les éléments suivants : $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ et $B = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix}$, où $j = e^{i\frac{2\pi}{3}}$.*

*On note $G =< A, B >$ le sous- groupe de $Gl_2(\mathbb{C})$ engendré par A et B.*

*1) Déterminer les ordres de A et de B.*

*2) Vérifier que $ABA^{-1} = B^2$ et que $AB^2A^{-1} = B$.*

*3) Montrer que $G = \{A^hB^k / h \in \{0, 1, 2, 3\}$ et $k \in \{0, 1, 2\}\}$.*

**Solution**

*1) $o(A) = 4$ ($A^2 = -I, A^3 = -A, A^4 = I$). $o(B) = 3$ ($B^2 = \begin{pmatrix} j^2 & 0 \\ 0 & j \end{pmatrix}$, $B^3 = I$).*

*2) On a $ABA^{-1} = ABA^3 = -ABA = \begin{pmatrix} j^2 & 0 \\ 0 & j \end{pmatrix} = B^2$. Aussi, $AB^2A^{-1} = (ABA^{-1})^2 = (-ABA)^2 = (B^2)^2 = B$.*

*3) Soit $M \in G$, alors $M = A^{m_1}B^{n_1}...A^{m_r}B^{n_r}$ avec $m_i, n_i \in \mathbb{Z}$ et $r \in \mathbb{N}^*$. Puisque $o(A) = 4$ et $o(B) = 3$ alors $M = A^{l_1}B^{s_1}...A^{l_r}B^{s_r}$ avec $l_i \in \{0,1,2,3\}$ et $s_i \in \{0,1,2\}$.*

*On a $BA = AB^2$ (question 2)), $B^2A = B(BA) = B(AB^2) = (BA)B^2 = AB^4 = AB$ et ainsi si $C = B^lA^s$ (avec $l \in \{1,2\}$ et $s \in \{1,2,3\}$ alors $C = A^uB^v$. (Par exemple, si $C = BA^2$, alors $C = (BA)A = (AB^2)A = A(B^2A) = A(AB) = A^2B$). Par suite, $M$ s'écrit sous la forme $M = A^hB^k$ avec $h \in \{0,1,2,3\}$ et $k \in \{0,1,2\}$.*

**Exercice 2.9** *Soit $G$ un groupe fini noté multiplicativement. Montrer que tout homomorphisme de groupes de $(\mathbb{Q},+)$ vers $(G,.)$ est triviale. i.e., si $f : \mathbb{Q} \longrightarrow G$ est un homomorphisme de groupes, alors $\forall x \in \mathbb{Q}, f(x) = e$. (Ind : remarquer que si $\frac{n}{m} \in \mathbb{Q}$, alors $f(s.\frac{n}{m}) = (f(\frac{n}{m}))^s$, $\forall s \in \mathbb{Z}$).*

**Solution**

*Soient $\frac{n}{m} \in \mathbb{Q}$ et $d$ l'ordre de $G$. Alors $f(\frac{n}{m}) = f(d\frac{n}{dm}) = (f(\frac{n}{dm}))^d$ et puisque $f(\frac{n}{dm}) \in G$ et $d$ est l'ordre de $G$, $(f(\frac{n}{dm}))^d = e$.*

**Exercice 2.10**

*1) Déterminer les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et l'image de $m\mathbb{Z}$ par la surjection canonique $s : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$.*

*Application : Déterminer les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ et les images de $5\mathbb{Z}$ et $8\mathbb{Z}$ par la surjection canonique $s : \mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$.*

*2) Montrer que si $q/n$, alors les groupes $q\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/\frac{n}{q}\mathbb{Z}$ sont isomorphes.*

**Solution**

*1) * Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $m\mathbb{Z}/n\mathbb{Z}$ tels que $m/n$.*

*** $s(m\mathbb{Z}) = m\mathbb{Z} + n\mathbb{Z}/n\mathbb{Z} = d\mathbb{Z}/n\mathbb{Z}$ où $d = n \wedge m$. En particulier, si $m/n$, alors $s(m\mathbb{Z}) = m\mathbb{Z}/n\mathbb{Z}$.*

*Application : Les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ sont de la forme $m\mathbb{Z}/12\mathbb{Z}$ tels que $m/12$. Ainsi, les sous-groupes de $\mathbb{Z}/12\mathbb{Z}$ sont $\mathbb{Z}/12\mathbb{Z}, 2\mathbb{Z}/12\mathbb{Z} =<\bar{2}>= \{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8},\overline{10}\}$, $3\mathbb{Z}/12\mathbb{Z} =<\bar{3}>= \{\bar{0},\bar{3},\bar{6},\bar{9}\}$, $4\mathbb{Z}/12\mathbb{Z} =<\bar{4}>= \{\bar{0},\bar{4},\bar{8}\}$, $6\mathbb{Z}/12\mathbb{Z} =<\bar{6}>= \{\bar{0},\bar{6}\}$ et $12\mathbb{Z}/12\mathbb{Z} = \{\bar{0}\}$.*

**** $s(5\mathbb{Z}) = (5 \wedge 12)\mathbb{Z}/12\mathbb{Z} = \mathbb{Z}/12\mathbb{Z}$ et $s(8\mathbb{Z}) = (8 \wedge 12)\mathbb{Z}/12\mathbb{Z} = 4\mathbb{Z}/12\mathbb{Z}$.*

*2) $\mathbb{Z}/n\mathbb{Z} =<\bar{1}>$ est un groupe cyclique d'ordre $n$. Puisque $q/n$, $q$ est le plus petit entier strictement positifs tel que $q.\bar{1} \in q\mathbb{Z}/n\mathbb{Z}$ et ainsi $q\mathbb{Z}/n\mathbb{Z} =<\bar{q}>$ est le sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre $\frac{n}{q}$ (cf. exercice 2.3)). Comme $q\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$, $q\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre $\frac{n}{q}$ et alors $q\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{q}\mathbb{Z}$.*

*Autre méthode : On peut aussi montrer que $q\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/\frac{n}{q}\mathbb{Z}$ en utilisant le premier théorème d'isomorphisme. En effet, soit $f : \mathbb{Z} \longrightarrow q\mathbb{Z}/n\mathbb{Z}$, $x \longmapsto \overline{qx}$. $f$ est évidemment un homomorphisme de groupes surjectif. Soit $x \in \mathbb{Z}$, $x \in \ker f$ si, et seulemet si, $\overline{qx} = \bar{0}$ si, et seulemet si, $n/qx$ si, et seulemet si, $\frac{n}{q}/x$ si, et seulemet si, $x \in \frac{n}{q}\mathbb{Z}$, ainsi $\ker f = \frac{n}{q}\mathbb{Z}$ et en appliquant le premier théorème d'isomorphisme, on obtient $\mathbb{Z}/\frac{n}{q}\mathbb{Z} \simeq q\mathbb{Z}/n\mathbb{Z}$.*

**Exercice 2.11** *Soient $G$ un groupe, $a \in G$ et $\tau_a : G \longrightarrow G$, $x \longmapsto axa^{-1}$ un automorphisme intérieur de $G$.*

*1) Vérifier que l'ensemble $Int(G)$ des automorphismes intérieurs de $G$ est un sous-groupe de $Aut(G)$.*

*2) Montrer que le centre $Z(G)$ de $G$ est un sous-groupe distingué de $G$ et que $G/Z(G) \simeq Int(G)$.*

**Solution**

*1) D'après le cours, on a $\forall a \in G$, $\tau_a \in Aut(G)$. Alors, soit l'application $f : G \longrightarrow Aut(G)$, $a \longmapsto \tau_a$. Vérifions que $f$ est un homomorphisme de groupes : on a $\forall x \in G$, $\tau_{ab}(x) = abxb^{-1}a^{-1} = a(bxb^{-1})a^{-1} = \tau_a(bxb^{-1}) = \tau_a \circ \tau_b(x)$ d'où $\forall a, b \in G$, $f(ab) = \tau_{ab} = \tau_a \circ \tau_b = f(a) \circ f(b)$. Puisque $Int(G) = f(G)$ et $f$ est un homomorphisme de groupes, alors $Int(G)$ est un sous-groupe de $Aut(G)$.*

*Autre méthode : On peut aussi vérifier que $Int(G)$ est un sous-groupe de $Aut(G)$ en utilisant la caractérisation des sous-groupes : $Int(G) \subset Aut(G)$, $Int(G) \neq \emptyset$ car $Id_G = \tau_e \in Int(G)$ et $\forall \tau_a, \tau_b \in G, \tau_a \circ (\tau_b)^{-1} = \tau_{ab^{-1}}$ car $(\tau_b)^{-1} = \tau_{b^{-1}}$ et $\tau_a \circ \tau_c = \tau_{ac}$.*

*2) On a $ker f = Z(G)$. En effet, soit $a \in G$, $a \in \ker f$ si, et seulemet si, $\tau_a = Id_G$ si, et seulemet si, $\forall x \in G, ax = xa$ si, et seulemet si, $a \in Z(G)$. Ainsi, $Z(G)$ est un sous-groupe distingué de $G$ et en appliquant le premier théorème d'isomorphisme, on obtient, $G/\ker f \simeq \operatorname{Im} f$, i.e., $G/Z(G) \simeq Int(G)$.*

**Exercice 2.12** *Soient $G$ un groupe et $Z(G)$ le centre de $G$. Montrer que si le groupe $G/Z(G)$ est monogène, alors $G$ est abélien.*

**Solution**

*Posons $G/Z(G) =< aZ(G) >$ . Soient $x, y \in G$, puisque $G/Z(G) =< aZ(G) >$, $\exists n, m \in \mathbb{Z} : xZ(G) = (aZ(G))^n = a^n Z(G)$, i.e., $x = a^n z_1$ avec $z_1 \in Z(G)$ et $yZ(G) = (aZ(G))^m = a^m Z(G)$, i.e., $y = a^m z_2$ avec $z_2 \in Z(G)$. Ainsi, $xy = a^n z_1 a^m z_2 = a^m z_2 a^n z_1 = yx$ car $z_1, z_2 \in Z(G)$ et $a^n a^m = a^{n+m} = a^m a^n$.*

**Exercice 2.13** *Soient $n, d \in \mathbb{N}^*$, $G$ un groupe abélien d'ordre $n$ noté multiplicativement et $f : G \longrightarrow G, x \longmapsto x^d$.*

*1) Montrer que $f$ est un endomorphisme de $G$.*

*2) Montrer que si $n \wedge d = 1$, alors $f$ est un automorphisme de $G$.*

*3) En déduire que si $n$ est impair, alors tout élément de $G$ est un carré.*

**Solution**

*1) On a $\forall x, y \in G$, $f(x.y) = (xy)^d = x^d y^d$ car $G$ est abélien. Alors $f(x.y) = f(x)f(y)$.*

*2) Puisque $G$ est fini et $f : G \longrightarrow G$ est une application de $G$ dans $G$, il suffit de vérifier que $f$ est injectif. Soit $x \in \ker f$, alors $f(x) = x^d = e$ d'où $\circ(x)/d$. D'autre part, $\circ(x)/n$ car $x \in G$ d'où $\circ(x)/n \wedge d = 1$ donc $\circ(x) = 1$ et ainsi $x = e$ d'où $\ker f = \{e\}$.*

*3) Posons $d = 2$, alors $n \wedge d = 1$ d'où $f : G \longrightarrow G$, $x \longmapsto x^2$ est un automorphisme de $G$ et ainsi $f$ est surjectif, i.e., $\forall g \in G$, $\exists x \in G : f(x) = x^2 = g$.*

**Exercice 2.14** *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 7 & 1 & 4 & 2 & 6 & 9 & 8 & 5 & 10 \end{pmatrix} \in S_{10}$.

*1) Décomposer $\sigma$ en produit de cycles disjoints et en produit de transpositions.*

*2) Déterminer $\varepsilon(\sigma)$.*

*3) Calculer $\sigma^{2007}$.*

**Solution**

*1)* $\sigma = (13)(2795)$ *est une décomposition de* $\sigma$ *en un produit de cycles disjoints et* $\sigma = (13)(27)(79)(95)$ *est une décomposition de* $\sigma$ *en un produit de transpositions.*

*2) Puisque* $\sigma$ *se décompose en un nombre pair de transpositions,* $\varepsilon(\sigma) = 1$.

*3) Puisque* $(13)$ *et* $(2795)$ *sont des cycles disjoints,* $(13)$ *et* $(2795)$ *commutent et ainsi* $\sigma^2 = (2795)^2 = (29)(75)$. *On a aussi* $\sigma^3 = (13)(2795)(29)(75) = (13)(2597)$, $\sigma^4 = (13)(2795)(13)(2597) = (2795)(2597) = e$ *et ainsi* $o(\sigma) = 4$.

*Comme* $2007 = 4.501 + 3$, $\sigma^{2007} = (\sigma^4)^{501}.\sigma^3 = e\sigma^3 = \sigma^3 = (13)(2597)$.

**Exercice 2.15**

*1) Déterminer tous les éléments de* $\mathcal{A}_4$.

*2) Soient* $c = (ijk)$ *un 3-cycle élément de* $S_4$ *et* $\sigma \in S_4$. *Calculer* $\sigma c \sigma^{-1}$.

*3) Montrer que* $\mathcal{A}_4$ *ne possède pas de sous-groupes d'ordre* 6.

**Solution**

*1)* $A_4 = \{e, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$. *On rappelle que* $|A_4| = \frac{|S_4|}{2} = \frac{24}{2} = 12$.

*2) On a* $\sigma(ijk)\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k))$. *En effet,* $\sigma(ijk)\sigma^{-1}(\sigma(i)) = \sigma(ijk)(i) = \sigma(j)$. *De même,* $\sigma(ijk)\sigma^{-1}(\sigma(j)) = \sigma(k)$ *et* $\sigma(ijk)\sigma^{-1}(\sigma(k)) = \sigma(i)$. *Si* $l \notin \{\sigma(i), \sigma(j), \sigma(k)\}$, *alors* $\sigma^{-1}(l) \notin \{i, j, k\}$ *d'où* $(ijk)(\sigma^{-1}(l)) = \sigma^{-1}(l)$, *ainsi* $\sigma(ijk)\sigma^{-1}(l) = \sigma\sigma^{-1}(l) = l$. *Alors* $\sigma(ijk)\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k))$.

*3) Supposons que* $A_4$ *possède un sous-groupe d'ordre 6 qu'on note* $H$. *Alors* $H$ *est distingué dans* $A_4$ *car* $[A_4 : H] = 2$. *D'autre part, puisque le nombre des éléments de* $A_4$ *qui ne sont pas des 3-cycles est 4, alors* $H$ *contient un 3-cycle qu'on note* $(ijk)$. *Alors* $(ikj) = (ijk)^2 \in H$.

*Soient* $l \notin \{i, j, k\}$ *et* $\sigma_1 = (ijl)$. *On a* $\sigma_1(ijk)\sigma_1^{-1} = (\sigma_1(i)\sigma_1(j)\sigma_1(k)) = (jlk) \in H$ *car* $H$ *est distingué dans* $A_4$ ($\sigma_1 \in A_4$ *et* $(ijk) \in H$) *et par suite* $(jkl) = (jlk)^2 \in H$. *De même, en considérant* $\sigma_2 = (ilj)$, *on a* $\sigma_2(ijk)\sigma_2^{-1} = (\sigma_2(i)\sigma_2(j)\sigma_2(k)) = (lik) \in H$ *et aussi* $(lki) = (lik)^2 \in H$.

*Ainsi, on obtient six 3-cycles distincts de* $H$. *Or* $e$ *est aussi un élément de* $H$, *contradiction.*

**Exercice 2.16**

*1) Soient* $G$ *un groupe,* $a$ *et* $b$ *deux éléments de* $G$ *d'ordre fini tels que* $ab = ba$ *et* $< a > \cap < b >= \{e\}$. *Montrer que* $o(ab) = o(a) \vee o(b)$.

*2)*

*a) Soit* $n > 2$ *un entier naturel pair et* $\sigma \in S_n : \sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 5, \sigma(4) = 6, \ldots, \sigma(n-3) = n-1, \sigma(n-2) =, \sigma(n-1) = 1, \sigma(n) = 2$. *Déterminer* $o(\sigma)$ *et* $\varepsilon(\sigma)$.

*b) Soit* $n > 3$ *un entier naturel impair et* $\sigma \in S_n : \sigma(1) = 3, \sigma(2) = 4, \sigma(3) = 5, \sigma(4) = 6, \ldots, \sigma(n-3) = n-1, \sigma(n-2) = n, \sigma(n-1) = 2, \sigma(n) = 1$. *Déterminer* $o(\sigma)$ *et* $\varepsilon(\sigma)$.

**Solution**

*1) Posons* $o(a) = n$, $o(b) = m$ *et* $o(ab) = k$. *Puisque* $(ab)^{n\vee m} = a^{n\vee m}b^{n\vee m} = e.e = e$, $o(ab)/n \vee m$. *D'autre part, on a* $(ab)^k = e$, *i.e.* $a^k = b^{-k}$ *et puisque* $a^k = b^{-k} \in < a > \cap < b >$, *alors* $a^k = b^{-k} = e$ *d'où* $n/k$ *et* $m/k$ *et ainsi* $n \vee m/k = o(ab)$.

*2)*

*a) * On a* $\sigma = c_1c_2$ *avec* $c_1 = (13...n-1)$ *et* $c_2 = (24...n)$. *Puisque les cycles* $c_1$ *et* $c_2$ *sont disjoints, alors* $c_1c_2 = c_2c_1$ *et* $< c_1 > \cap < c_2 >= \{e\}$ *et ainsi* $o(\sigma) = o(c_1) \vee o(c_2) = \frac{n}{2}$ $(o(c_1) = o(c_2) = \frac{n}{2})$.

** $\varepsilon(\sigma) = \varepsilon(c_1c_2) = \varepsilon(c_1)\varepsilon(c_2) = (-1)^{\frac{n}{2}-1}(-1)^{\frac{n}{2}-1} = 1$. *On rappelle que si* $c$ *est un cycle de longueur* $k$, *alors* $\varepsilon(c) = (-1)^{k-1}$.

*b) * On a* $\sigma = c_1c_2$ *avec* $c_1 = (13...n)$ *et* $c_2 = (24...n-1)$. *Puisque les cycles* $c_1$ *et* $c_2$ *sont disjoints, alors* $c_1c_2 = c_2c_1$ *et* $< c_1 > \cap < c_2 >= \{e\}$ *et ainsi* $o(\sigma) = o(c_1) \vee o(c_2) = \frac{n+1}{2} \vee \frac{n-1}{2} = \frac{(n-1)(n+1)}{4}$ $(o(c_1) = \frac{n+1}{2}, o(c_2) = \frac{n-1}{2}$, $\frac{n-1}{2}$ *et* $\frac{n+1}{2}$ *sont premiers entre eux)*.

** $\varepsilon(\sigma) = \varepsilon(c_1c_2) = \varepsilon(c_1)\varepsilon(c_2) = (-1)^{\frac{n+1}{2}-1}(-1)^{\frac{n-1}{2}-1} = -1$.

# Chapitre 3

# Anneaux et corps

Tous les anneaux sont supposés être unitaires et non triviaux.

**Exercice 3.1** *Soit $A$ un anneau commutatif, $I$ et $J$ deux idéaux de $A$. On considère $(I : J) = \{a \in A : aJ \subset I\}$.*

*1) Montrer que $(I : J)$ est un idéal de $A$ contenant $I$.*

*2) Montrer que $(I : J)J \subset I$.*

*3) Montrer que si $K$ est un idéal de $A$, alors $(I \cap J : K) = (I : K) \cap (J : K)$ et que $(I : J + K) = (I : J) \cap (I : K)$.*

**Solution**

*1) * Montrons que $(I : J) = \{a \in A : aJ \subset I\}$ est un idéal de $A$. On a $(I : J) \subset A$, $(I : J) \neq \emptyset$ car $0 \in (I : J)$. $\forall x, y \in (I : J)$, $\forall j \in J$, on a $(x-y)j = xj-yj$ et puisque $xj, yj \in I$ et $I$ est un idéal de $A$, $(x-y)j \in I$ d'où $(x-y) \in (I : J)$. On a aussi $\forall a \in A, \forall x \in (I : J)$, $axJ = a(xJ)$ et puisque $xJ \subset I$ et $I$ est un idéal de $A$, $axJ \subset I$ alors $(I : J)$ est un idéal de $A$.*

** On a $I \subset (I : J)$. En effet, $\forall i \in I$, $iJ \subset I$ car $I$ est un idéal de $A$.*

*2) Comme $(I : J)J$ est l'idéal de $A$ engendré par l'ensemble $\{xy/x \in (I : J)$ et $y \in J\}$, il suffit de vérifier que $\{xy/x \in (I : J)$ et $y \in J\} \subset I$. Soit $x \in (I : J)$ et $y \in J$, alors $xy \in I$.*

*3) * Soit $x \in A$. $x \in (I \cap J : K)$ si, et seulement si, $xK \subset I$ et $xK \subset J$, i.e., $x \in (I : K) \cap (J : K)$.*

** Si $x \in (I : J + K)$ alors $x(J + K) \subset I$ d'où $xJ + xK \subset I$ et comme $xJ \subset xJ + xK \subset I$ (resp.$xK \subset xJ + xK \subset I$), $x \in (I : J) \cap (I : K)$. Pour l'autre inclusion, soit $x \in (I : J) \cap (I : K)$, alors $xJ \subset I$ et $xK \subset I$ d'où $xJ + xK \subset I$, ainsi $x \in (I : J + K)$.*

**Exercice 3.2** *Soient $A$ un anneau commutatif, $I_1, ..., I_n$ des idéaux de $A$.*

*1) Vérifier que $I_1.(I_2.I_3) = (I_1.I_2).I_3$*

*2) On définit par récurrence l'idéal $I_1...I_n$ en posant $I_1.I_2.I_3 = (I_1.I_2).I_3, ..., I_1...I_n = (I_1...I_{n-1})I_n$. Montrer que si $I_1 = (a_1), ..., I_n = (a_n)$, alors $I_1...I_n = (a_1...a_n)$. En déduire que $I^n = (a^n)$ si $I = (a)$.*

**Solution**

*1) Il suffit de vérifier que $I_1.(I_2.I_3)$ et $(I_1.I_2).I_3$ sont (tous les deux) engendrés par l'ensemble $X = \{xyz/x \in I_1, y \in I_2, z \in I_3\}$. On a $X \subset I_1.(I_2.I_3)$. Soit $J$ un idéal contenant $X$. Montrons que $I_1.(I_2.I_3) \subset J$. D'après le cours, $I_1.(I_2.I_3)$ est engendré par l'ensemble $\{uv : u \in I_1$ et $v \in (I_2.I_3)\}$. Ainsi, pour montrer que $I_1.(I_2.I_3) \subset J$, il suffit de vérifier que $\{uv : u \in I_1$*

*et* $v \in (I_2.I_3)\} \subset J$. *Soit* $uv$ *tel que* $u \in I_1$ *et* $v \in (I_2.I_3)$, *on a* $v = \sum_{i=1}^{n} y_i z_i$, *avec* $n \in \mathbb{N}^*$, $y_i \in I_2, z_i \in I_3$ *d'où* $uv = \sum_{i=1}^{n} u\,y_i z_i$. *Puisque* $uy_iz_i \in X \subset J$ *et* $J$ *est un idéal,* $uv \in J$.

*De la même façon, on montre que* $(I_1.I_2).I_3$ *est engendré par* $X$. *Donc* $I_1.(I_2.I_3) = (I_1.I_2).I_3$.

*2) D'après la définition de* $I_1...I_n$, $I_1...I_n$ *est l'ensemble des sommes finies d'éléments de la forme* $x_1...x_n$, *avec* $x_i \in I_i$. *Alors* $a_1...a_n \in I_1...I_n$ *et par suite* $(a_1...a_n) \subset I_1...I_n$. *Pour l'autre inclusion, soit* $x \in I_1...I_n$, *alors* $x$ *s'écrit comme somme finie d'éléments de la forme* $x_1...x_n$, *avec* $x_i \in I_i$. *Comme* $x_1...x_n = (\beta_1 a_1)...(\beta_n a_n)$ , *avec* $\beta_i \in A$, $x_1...x_n = (\beta_1...\beta_n)a_1...a_n \in (a_1...a_n)$ *d'où* $x \in (a_1...a_n)$.

*Ainsi, si* $I = (a)$, *alors* $I^n = I...I = (a...a) = (a^n)$.

**Exercice 3.3** *Soient* $A$ *un anneau,* $I, J$ *deux idéaux de* $A$, $\mathfrak{p}$ *un idéal premier de* $A$ *et* $\mathfrak{m}$ *un idéal maximal de* $A$.

*1) Montrer que si* $IJ \subset \mathfrak{p}$, *alors* $I \subset \mathfrak{p}$ *ou* $J \subset \mathfrak{p}$ *et que si* $I \cap J = \mathfrak{p}$ *alors* $\mathfrak{p} = I$ *ou* $\mathfrak{p} = J$.

*2) En déduire que le seul idéal premier de* $A$ *qui contient* $\mathfrak{m}^2$ *est l'idéal* $\mathfrak{m}$.

**Solution**

*1) * Supposons que* $I \not\subset \mathfrak{p}$, *i.e.,* $\exists x \in I : x \notin \mathfrak{p}$. *Montrons que* $J \subset P$ : $\forall y \in J$, *on a* $xy \in IJ \subset \mathfrak{p}$ *et comme* $\mathfrak{p}$ *est premier et* $x \notin \mathfrak{p}$, $y \in \mathfrak{p}$.

** Si* $I \cap J = \mathfrak{p}$, *alors* $IJ \subset I \cap J = \mathfrak{p}$ *d'où* $I \subset \mathfrak{p}$ *ou* $J \subset \mathfrak{p}$ *et comme* $\mathfrak{p} \subset I$ *et* $\mathfrak{p} \subset J$ *car* $I \cap J = \mathfrak{p}$, *alors* $\mathfrak{p} = I$ *ou* $\mathfrak{p} = J$.

*2) On a* $\mathfrak{m}^2 \subset \mathfrak{m}$ *et* $\mathfrak{m}$ *est premier car* $\mathfrak{m}$ *est maximal. Montrons que c'est le seul idéal premier de* $A$ *qui contient* $\mathfrak{m}^2$. *Soit* $\mathfrak{p}$ *un idéal premier tel que* $\mathfrak{m}^2 \subset \mathfrak{p}$, *alors d'après 1)* $\mathfrak{m} \subset \mathfrak{p}$ *et puisque* $\mathfrak{m}$ *est maximal et* $\mathfrak{p} \neq A$ *car* $\mathfrak{p}$ *est premier,* $\mathfrak{m} = \mathfrak{p}$.

**Exercice 3.4** *Soient A,B deux anneaux et* $f : A \longrightarrow B$ *un homomorphisme d'anneaux.*

*1)*

*a) Donner un exemple d'un idéal* $I$ *de* $A$ *tel que* $f(I)$ *n'est pas un idéal de* $B$.

*b) Montrer que si* $f$ *est surjectif, alors* $f(I)$ *est un idéal de* $A$.

*2) Montrer que si* $\mathfrak{p}$ *est un idéal premier de* $B$, *alors* $f^{-1}(\mathfrak{p})$ *est un idéal premier de* $A$.

*3) Donner un exemple d'un idéal maximal* $\mathfrak{m}$ *de* $B$ *tel que* $f^{-1}(\mathfrak{m})$ *n'est pas un idéal maximal de* $A$.

**Solution**

*1)*

*a) On prend* $i : \mathbb{Z} \longrightarrow \mathbb{Q}, a \longmapsto a$, $i$ *est un homomorphisme d'anneaux,* $2\mathbb{Z}$ *est un idéal de* $\mathbb{Z}$, *mais* $i(2\mathbb{Z}) = 2\mathbb{Z}$ *n'est pas un idéal de* $\mathbb{Q}$.

*b)* $(I, +)$ *est un sous-groupe de* $(A, +)$ *et* $f$ *est un homomorphisme de groupes de* $(A, +)$ *vers* $(B, +)$ *d'où* $f(I)$ *est un sous-groupe de* $(B, +)$. *On a aussi* $\forall b \in B, \forall y \in f(I)$, $b = f(a)$, *où* $a \in A$ *car* $f$ *est surjectif et* $y = f(x)$, *avec* $x \in I$. *Alors,* $by = f(a).f(x) = f(ax)$ *et puisque* $ax \in I$ *car* $I$ *est un idéal de* $A$, $by \in f(I)$.

*2) D'après le cours,* $f^{-1}(\mathfrak{p})$ *est un idéal de* $A$. *Montrons que* $f^{-1}(\mathfrak{p})$ *est premier. On a* $f^{-1}(\mathfrak{p}) \neq A$, *sinon* $1_A \in f^{-1}(\mathfrak{p})$ *et par suite* $1_B = f(1_A) \in \mathfrak{p}$, *i.e.,* $\mathfrak{p} = B$. *Soient* $a, b \in A$ : $ab \in f^{-1}(\mathfrak{p})$, *d'où* $f(ab) = f(a)f(b) \in \mathfrak{p}$ *alors* $f(a) \in \mathfrak{p}$ *ou* $f(b) \in \mathfrak{p}$ *et ainsi* $a \in f^{-1}(\mathfrak{p})$ *ou* $b \in f^{-1}(\mathfrak{p})$.

*3) Soit* $i : \mathbb{Z} \longrightarrow \mathbb{Q}, a \longmapsto a$. $(0)$ *est un idéal maximal de* $\mathbb{Q}$*, mais* $(0) = i^{-1}(0)$ *n'est pas un idéal maximal de* $\mathbb{Z}$.

**Exercice 3.5**

*1) Soit* $n \in \mathbb{N} - \{0,1\}$. *Déterminer* $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ *et* $|\mathcal{U}(\mathbb{Z}/n\mathbb{Z})|$.

*2) Soient* $A, B$ *deux anneaux. Montrer que* $\mathcal{U}(A \times B) = \mathcal{U}(A) \times \mathcal{U}(B)$.

*3) Montrer que si* $m, n \in \mathbb{N} - \{0,1\} : m \wedge n = 1$*, alors* $\varphi(nm) = \varphi(n).\varphi(m)$. *(ind : utiliser* $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*).*

*4) Soit* $n \in \mathbb{N} - \{0,1\}$. *Calculer* $\varphi(n)$. *(Ind : écrire* $n = p_1^{\alpha_1}.\dots.p_r^{\alpha r}$*, avec* $p_i$ *premiers,* $p_i \neq p_j$ *si* $i \neq j, \alpha_i \neq 0$*, calculer* $\varphi(p^m)$ *si* $p$ *est premier et utiliser 3)).*

**Solution**

*1) Soit* $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$*,* $\bar{m} \in \mathcal{U}(\mathbb{Z}/n\mathbb{Z})$ *si, et seulement si,* $\exists \bar{l} \in \mathbb{Z}/n\mathbb{Z} : \bar{m}.\bar{l} = \bar{1}$ *si, et seulement si,* $\exists k \in \mathbb{Z} : 1 = kn + ml$ *si, et seulement si,* $m \wedge n = 1$. *Ainsi,* $|\mathcal{U}(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)$.

*2) Soit* $(a,b) \in A \times B$. $(a,b) \in \mathcal{U}(A \times B)$ *si, et seulement si,* $\exists (a', b') \in A \times B : (a,b).(a',b') = (aa', bb') = (1,1)$ *si, et seulement si,* $(a,b) \in \mathcal{U}(A) \times \mathcal{U}(B)$.

*3) Soient* $m, n \in \mathbb{N} - \{0,1\} : m \wedge n = 1$. *D'après le cours,* $\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ *d'où* $\mathcal{U}(\mathbb{Z}/nm\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})$ *(en tant que groupes), alors* $\mathcal{U}(\mathbb{Z}/nm\mathbb{Z}) \simeq \mathcal{U}(\mathbb{Z}/n\mathbb{Z}) \times \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$ *et ainsi* $\varphi(nm) = |\mathcal{U}(\mathbb{Z}/nm\mathbb{Z})| = |\mathcal{U}(\mathbb{Z}/n\mathbb{Z})|.|\mathcal{U}(\mathbb{Z}/m\mathbb{Z})| = \varphi(n).\varphi(m)$.

*4) Soient* $p$ *un nombre premier,* $m \in \mathbb{N}^*$ *et* $l \in \{1, ..., p^m\}$. *Alors,* $l \wedge p^m \neq 1$ *si, et seulement si,* $p/l$. *Or les multiples de* $p$ *dans* $\{1, ..., p^m\}$ *sont* $p, 2p, ..., p^{m-1}p = p^m$ *et leur nombre est* $p^{m-1}$ *d'où* $\varphi(p^m) = p^m - p^{m-1}$.

*Si* $n = p_1^{\alpha_1}.\dots.p_r^{\alpha r}$ *avec* $p_i$ *premiers,* $p_i \neq p_j$ *si* $i \neq j, \alpha_i \neq 0$*, alors, d'après 3),* $\varphi(n) = \varphi(p_1^{\alpha_1})...\varphi(p_r^{\alpha_r})$ *car* $p_i^{\alpha_i} \wedge p_j^{\alpha_j} = 1$ *si* $i \neq j$*, et ainsi* $\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})...(p_r^{\alpha_r} - p_r^{\alpha_r - 1}) = n(1 - \frac{1}{p_1})...(1 - \frac{1}{p_r})$.

**Exercice 3.6**

*1) Soit* $K = \{\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} / a \in \mathbb{R}\}$. *Montrer que* $K$*, muni de l'addition et de la multiplication des matrices, est un corps.* $K$ *est-il un sous-anneau (au sens des anneaux unitaires) de l'anneau* $M_2(\mathbb{R})$*?*

*2) Soit* $A = \{\begin{pmatrix} a & 0 \\ b & a \end{pmatrix} / a, b \in \mathbb{Z}\}$.

*a) Montrer que* $A$ *est un sous-anneau commutatif de* $\mathcal{M}_2(\mathbb{R})$.

*b) Montrer que* $I = \{\begin{pmatrix} 0 & 0 \\ b & 0 \end{pmatrix} / b \in \mathbb{Z}\}$ *est un idéal premier de* $A$. $I$ *est-il maximal ?*

**Solution**

*1) Il est évidnt que* $(K, +, .)$ *est un anneau commutatif. La matrice* $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ *est l'unité de* $K$ *et tout élément* $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \in K - \{0\}$ *est inversible et son inverse est* $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{a} \end{pmatrix}$. *Ainsi* $(K, +, .)$ *est un corps (commutatif).*

$K$ *n'est pas un sous-anneau (au sens des anneaux unitaires) de* $M_2(\mathbb{R})$ *car* $1_{M2(R)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin K$.

*2)*

*a) On vérifie facilement que* $A \neq \emptyset$, $I_2 \in A$, $\forall X, Y \in A, X - Y \in A$ *et* $XY \in A$.

*b) Soit* $f : A \longrightarrow \mathbb{Z}, \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} \longmapsto a$. *Il est évident que* $f$ *est un homomorphisme d'anneaux surjectif et que* $ker f = I$. *Ainsi, d'après le premier théorème d'isomorphisme,* $A/I \simeq \mathbb{Z}$ *et comme* $\mathbb{Z}$ *est intègre,* $I$ *est premier. Cependant,* $I$ *n'est pas un idéal maximal car* $\mathbb{Z}$ *n'est pas un corps.*

**Exercice 3.7**

*1) Soient* $A$ *et* $B$ *deux anneaux de caractéristiques respectivement* $m$ *et* $n$. *Montrer que* $car(A \times B) = n \vee m$.

*2) Soit* $A$ *un anneau intègre fini de caractéristique* $p$.

*a) Montrer que* $p \neq 0$.

*b) Montrer que* $A$ *peut être muni d'une structure d'espace vectoriel sur* $\mathbb{Z}/p\mathbb{Z}$. *En déduire que* $card(A) = p^n$, *où* $n \in \mathbb{N}^*$.

**Solution**

*1) Remarquons d'abord que si* $n = 0$ *ou* $m = 0$, *alors* $\forall k \in \mathbb{N}^*$, $k(1,1) \neq (0,0)$ *et ainsi* $car(A \times B) = 0$.

*Supposons maintenant que* $n \neq 0$ *et* $m \neq 0$. *On a* $(n \vee m).(1,1) = ((n \vee m)1, (n \vee m)1) = (0,0)$ *car* $n \vee m$ *est un multiple de* $n$ *et de* $m$. *D'où* $car(A \times B) \neq 0$. *Posons* $s = car(A \times B)$. *Alors, d'après le cours,* $s = \circ(1,1)$ *(*$(1,1)$ *est considéré comme élément du groupe additif* $(A \times B, +)$*). Comme* $(n \vee m).(1,1) = (0,0)$, $s/n \vee m$. *D'autre part, on a* $s(1,1) = (s1, s1) = (0,0)$, *d'où* $n/s$ *et* $m/s$ *et ainsi* $n \vee m/s$.

*2) Puisque* $A$ *est intègre et d'après le cours,* $p = 0$ *ou* $p$ *est premier.*

*a) Comme* $(A, +)$ *est un groupe fini,* $\circ(1)$ *est fini et ainsi* $car(A) = p \neq 0$.

*b)* $\mathbb{Z}/p\mathbb{Z}$ *est un corps (commutatif) et* $(A, +)$ *est un groupe abélien. Soit* $\cdot : \mathbb{Z}/p\mathbb{Z} \times A \longrightarrow A, (\bar{k}, a) \longmapsto ka$. $\cdot$ *est une application bien définie. En effet, soient* $(\bar{k}_1, a) = (\bar{k}_2, a)$ $(k_1, k_2 \in \{0, 1, ..., p-1\})$ *d'où* $p/k_1 - k_2$ *et donc* $(k_1 - k_2)1 = 0$ $(car A = p)$. *Puisque* $|k_1 - k_2| < p$, $k_1 - k_2 = 0$ *et ainsi* $k_1 a = k_2 a$.

*On vérifie facilement que* $A$, *muni de l'addition et de l'opération externe* $\cdot$, *est un* $\mathbb{Z}/p\mathbb{Z}$*-espace vectoriel.*

*Puisque* $A$ *est fini,* $A$ *est un espace vectoriel de dimension finie. Soient* $(u_1, ..., u_n)$ *une base de* $A$. *Alors, le nombre des éléments de* $A$ *est égal au nombre des combinaisons linéaires de la forme* $\overline{\alpha_1}u_1 + ... + \overline{\alpha_1}u_n$ *avec* $(\overline{\alpha_1}, ..., \overline{\alpha_n}) \in (\mathbb{Z}/p\mathbb{Z})^n$ *et ainsi* $card A = p^n$.

**Exercice 3.8** *Déterminer le corps des fractions de l'anneau* $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5}/a, b \in \mathbb{Z}\}$.

**Solution**

$Fr(\mathbb{Z}[\sqrt{5}]) = \{\frac{a+b\sqrt{5}}{c+d\sqrt{5}}/a, b, c, d \in \mathbb{Z}$ *et* $(c,d) \neq (0,0)\}$. *Soit* $x = \frac{a+b\sqrt{5}}{c+d\sqrt{5}} \in Fr(\mathbb{Z}[\sqrt{5}]$, $x = \frac{(a+b\sqrt{5})(c-d\sqrt{5})}{(c^2-5d^2)}$. *On a* $c - d\sqrt{5} \neq 0$ *car* $(c,d) \neq (0,0)$. *D'où* $x = \frac{(ac-5bd)}{(c^2-5d^2)} + \frac{(bc-ad)}{(c^2-5d^2)}\sqrt{5} \in \mathbb{Q}[\sqrt{5}] = \{\alpha + \beta\sqrt{5}/\alpha, \beta \in \mathbb{Q}\}$.

*Pour l'autre inclusion,* $\forall \alpha + \beta\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$, $\alpha + \beta\sqrt{5} = \frac{a}{b} + \frac{c}{d}\sqrt{5}$ *avec* $a, c \in \mathbb{Z}$ *et* $b, d \in \mathbb{Z}^*$ $(\alpha = \frac{a}{b}, \beta = \frac{c}{d})$. *Alors,* $\alpha + \beta\sqrt{5} = \frac{ad+bc\sqrt{5}}{bd} \in Fr(\mathbb{Z}[\sqrt{5}])$. *Ainsi,* $Fr(\mathbb{Z}[\sqrt{5}]) = \mathbb{Q}[\sqrt{5}]$ $(= \mathbb{Q}(\sqrt{5}))$.

# Chapitre 4

# Divisibilité dans un anneau principal

**Exercice 4.1** *On considère l'anneau* $\mathbb{Z}[i] = \{a + ib/\ a, b \in \mathbb{Z}\}$.

*1) Déterminer* $\mathcal{U}(\mathbb{Z}[i])$ *et* $Fr(\mathbb{Z}[i])$.

*2) On considère l'application* $f : \mathbb{Z}[i] \longrightarrow \mathbb{Z}/10\mathbb{Z},\ a + ib \longmapsto \overline{a + 7b}$.

*a) Montrer que* $f$ *est un homomorphisme d'anneaux surjectif.*

*b) Montrer que* $\ker f = (3 + i)$.

*c) En déduire que* $\mathbb{Z}[i]/(3 + i) \simeq \mathbb{Z}/10\mathbb{Z}$.

*d)* $3 + i$ *est -il premier dans* $\mathbb{Z}[i]$ *?*

**Solution**

*1)* Soit* $x = a+ib \in \mathcal{U}(\mathbb{Z}[i])$, *alors* $\exists\ y = c+id \in \mathbb{Z}[i]$ *tel que* $xy = 1$ *d'où* $|xy|^2 = |x|^2\,|y|^2 = 1$, *i.e.*$(a^2+b^2)(c^2+d^2) = 1$ *et par suite* $a^2+b^2 = 1$ $(a, b, c, d \in \mathbb{Z})$ *alors nécessairement* $a = \pm 1$ *ou bien* $b = \pm 1$ *donc* $\mathcal{U}(\mathbb{Z}[i]) \subset \{-1, 1, i, -i\}$. *D'autre part, on a* $\{-1, 1, i, -i\} \subset \mathcal{U}(\mathbb{Z}[i])$. *Ainsi* $\mathcal{U}(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$.

** On a* $Fr(\mathbb{Z}[i]) = \{\frac{x}{y}/\ x \in \mathbb{Z}[i],\ y \in (\mathbb{Z}[i])^*\}$. *Soit* $\frac{x}{y} \in Fr(\mathbb{Z}[i])$, *alors, en posant* $x = a + ib$, $y = c + id$ $((c, d) \neq (0, 0))$, *on a* $\frac{x}{y} = \frac{a+ib}{c+id} = \frac{(ac+bd)+i(bc-ad)}{c^2+d^2}$, $(c - id \neq 0)$, *d'où* $x = \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2} \in \mathbb{Q}[i] = \{\alpha + i\beta/\ \alpha, \beta \in \mathbb{Q}\}$ *et ainsi* $Fr(\mathbb{Z}[i]) \subset \mathbb{Q}[i]$. *On a aussi* $\mathbb{Q}[i] \subset Fr(\mathbb{Z}[i])$ *; en effet, soit* $z = \alpha + i\beta \in \mathbb{Q}[i]$ *alors* $\alpha = \frac{a}{b}$ *et* $\beta = \frac{c}{d}$, *avec* $a, c \in \mathbb{Z}, b, d \in \mathbb{Z}^*$ $(\alpha, \beta \in \mathbb{Q})$, *alors* $z = \frac{a}{b} + i\frac{c}{d} = \frac{ad+ibc}{bd} \in Fr(\mathbb{Z}[i])$. *Ainsi* $Fr(\mathbb{Z}[i]) = \mathbb{Q}[i]$.

*2)*

*a) Montrons que* $f$ *est un homomorphisme d'anneaux : soient* $x = a+ib, y = c+id \in \mathbb{Z}[i]$, *on a* $f(x+y) = f((a+c)+i(b+d)) = \overline{(a+c)+7(b+d)} = \overline{(a+7b)} + \overline{(c+7d)} = f(x)+f(y)$. *Aussi,*$f(xy) = f((a+ib)(c+id)) = f((ac-bd)+i(ad+bc)) = \overline{(ac-bd)+7(ad+bc)} = \overline{(ac+49bd)+7(ad+bc)} = \overline{(a+7b)(c+7d)} = f(x)f(y)$ *car* $\overline{-1} = \overline{49} \pmod{10}$) *; on a* $f(1) = \bar{1}$ *et ainsi* $f$ *est un homomorphisme d'anneaux.*

$f$ *est aussi surjectif. En effet, soit* $\bar{y} \in \mathbb{Z}/10\mathbb{Z}$, *alors* $\exists\ x = y \in \mathbb{Z}$ *tel que* $f(x) = \bar{x} = \bar{y}$.

*b) Montrons que* $\ker f = (3 + i)$ *: on a* $(3 + i) \subset \ker f$ *; en effet,* $f(3 + i) = \overline{3 + 7 \times 1} = \bar{0}$ *d'où* $3 + i \in \ker f$ *et par suite* $(3 + i) \subset \ker f$. *On a aussi* $\ker f \subset (3 + i)$ *En effet,*

$1^{\text{ère}}$ *méthode : Soit* $x = a + ib \in \ker f$ *alors* $f(x) = \overline{a + 7b} = \bar{0}$ *d'où* $\exists\ k \in \mathbb{Z}$ *tel que* $a + 7b = 10k$ *ainsi* $x = (10k - 7b) + ib = 10k + (i - 7)b = (3 + i)(3 - i)k + (i + 3)(i - 2)b$ *(* $10 = (3 + i)(3 - i)$ *et* $i - 7 = (i + 3)(i - 2)$*) alors* $x = (i + 3)((3 - i)k + (i - 2)b) = (i+3)((3k-2b)+i(b-k)) \in (i+3)$ *(car* $(3k-2b)+i(b-k) \in \mathbb{Z}[i]$*) et ainsi* $\ker f \subset (3+i)$.

$2^{\text{ème}}$ *méthode : Soit* $x = a + ib \in \ker f$, *alors* $f(x) = \overline{a + 7b} = \bar{0}$ *d'où* $\exists\ k \in \mathbb{Z}$ *tel que* $a + 7b = 10k$ *d'où* $x = 10k - 7b + ib$ *alors* $x = (i + 3)((3k - 2b) + i(b - k)) \in (i + 3)$ *et ainsi* $\ker f \subset (i + 3)$. *Pour chercher* $(3k - 2b) + i(b - k)$, *on procède comme suit : supposons*

*qu'il existe* $y = c + id \in \mathbb{Z}[i]$ *tel que* $x = 10k - 7b + ib = (i+3)y = (i+3)(c+id)$ *alors* $\begin{cases} 3c - d = & 10k - 7b \\ c + 3d = & b \end{cases}$ *d'où* $c = 3k - 2b$ *et* $d = b - k$ *et ainsi* $y = c + id = (3k-2b) + i(b-k)$ *; en multipliant* $(i+3)$ *par* $y$*, on obtient* $x$*.*

*c) D'après le premier théorème d'isomorphisme, on a* $\mathbb{Z}[i]/\ker f \simeq \operatorname{Im} f$*.* $\operatorname{Im} f = \mathbb{Z}/10\mathbb{Z}$ *car* $f$ *est surjectif et* $\ker f = (i+3)$*, alors* $\mathbb{Z}[i]/(i+3) \simeq \mathbb{Z}/10\mathbb{Z}$*.*

*d) L'anneau* $\mathbb{Z}/10\mathbb{Z}$ *n'est pas intègre car 10 n'est pas premier, alors* $\mathbb{Z}[i]/(i+3)$ *n'est pas intègre d'où l'idéal* $(i+3)$ *n'est pas un idéal premier et ainsi l'élément* $i+3$ *n'est pas premier.*

**Exercice 4.2**

*1) Soient* $A$ *un anneau intègre et* $a, b \in A - \{0\}$ *ayant un ppcm noté* $m$*. Montrer qu'il existe* $d \in A$ *tel que* $ab = md$ *et que* $d$ *est un pgcd de* $a$ *et* $b$*.*

*2) Soit l'anneau* $\mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}/a, b \in \mathbb{Z}\}$*.*

*a) Déterminer* $\mathcal{U}(\mathbb{Z}[i\sqrt{5}])$*.*

*b) Déterminer tous les diviseurs de* $9$ *et de* $3(2+i\sqrt{5})$*.*

*c) Montrer que* $1$ *est un pgcd de* $3$ *et* $2+i\sqrt{5}$ *et que* $3$ *et* $2+i\sqrt{5}$ *n'ont pas de ppcm. Conclure.*

*d) Montrer que les éléments* $9$ *et* $3(2+i\sqrt{5})$ *n'ont pas de pgcd dans* $\mathbb{Z}[i\sqrt{5}]$*.* $9$ *et* $3(2+i\sqrt{5})$ *admettent-ils un ppcm ?*

*e) Montrer que l'idéal engendré par* $3$ *et* $2+i\sqrt{5}$ *n'est pas principal.*

**Solution**

*1) Puisque* $a/ab$ *et* $b/ab$*, alors* $m/ab$*, i.e.,* $\exists d \in A : ab = md$*. On a* $d = a \wedge b$*. En effet,* $a/m$ *et* $b/m$ *d'où* $\exists \alpha, \beta \in A : m = \alpha a$ *et* $m = \beta b$*. Ainsi,* $ab = md = \alpha ad$ *(resp.* $ab = \beta bd$*). Puisque* $A$ *est intègre et* $a \neq 0$ *(resp.* $b \neq 0$*),* $b = \alpha d$ *(resp.* $a = \beta d$*), alors* $d/b$ *et* $d/a$*. D'autre part, soit* $c \in A : c/a$ *et* $c/b$*, alors* $a = cu$ *et* $b = cv$*. Comme* $a/cuv$ *et* $b/cuv$*,* $m/cuv$*, i.e.* $\exists t \in A : cuv = mt$ *d'où* $cuv = \alpha at$ *et* $v = \alpha t$ *car* $cu = a$*,* $a \neq 0$ *et* $A$ *est intègre. Puisque* $acv = ab = md = \alpha ad$*,* $cv = \alpha d$ *car* $a \neq 0$ *et* $A$ *est intègre et ainsi* $cv = c\alpha t = \alpha d$ *d'où* $ct = d$ *car* $\alpha \neq 0$ *et* $A$ *est intègre.*

*2)*

*a) Soit* $x = a + ib\sqrt{5} \in \mathcal{U}(\mathbb{Z}[i\sqrt{5}])$*, alors* $\exists y = c + id\sqrt{5} \in \mathbb{Z}[i\sqrt{5}] : xy = 1$*. En passant aux modules des complexes, on obtient* $(a^2+5b^2)(c^2+5d^2) = 1$ *d'où* $a^2 + 5b^2 = 1$ *(car* $a^2 + 5b^2 \in \mathbb{N}$*). Ainsi,* $a = \pm 1$ *et* $b = 0$*, i.e.* $x = \pm 1$*. D'autre part,* $\{-1, 1\} \subset \mathcal{U}(\mathbb{Z}[i\sqrt{5}])$*, alors* $\mathcal{U}(\mathbb{Z}[i\sqrt{5}]) = \{-1, 1\}$*.*

*b) Soit* $x = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$*. Si* $x/9$*, alors* $\exists y = c + id\sqrt{5} \in \mathbb{Z}[i\sqrt{5}] : xy = 9$*. En passant aux modules des complexes, on obtient* $(a^2+5b^2)(c^2+5d^2) = 81$*. Puisque* $a^2 + 5b^2 \neq 3$ *et* $a^2 + 5b^2 \neq 27$*,* $a^2 + 5b^2 \in \{1, 9, 81\}$*. Si* $a^2 + 5b^2 = 1$ *alors* $x = \pm 1$*. Aussi, si* $a^2 + 5b^2 = 81$*, i.e.* $c^2 + 5d^2 = 1$*, alors* $x = \pm 9$ *et si* $a^2 + 5b^2 = 9$*, alors (*$a = \pm 3$ *et* $b = 0$*) ou (*$a = \pm 2$ *et* $b = \pm 2$*).i.e,* $x = \pm 3$ *ou* $x = \pm(2+i\sqrt{5})$ *ou* $x = \pm(2-i\sqrt{5})$*. On vérifie facilement que* $\pm 1, \pm 9, \pm 3$*,* $\pm(2+i\sqrt{5})$ *et* $\pm(2-i\sqrt{5})$ *sont des diviseurs de 9. Ainsi, les diviseurs de 9 sont* $\pm 1, \pm 9, \pm 3$*,* $\pm(2+i\sqrt{5})$ *et* $\pm(2-i\sqrt{5})$*.*

*De même, on montre que si* $x/3(2+i\sqrt{5})$*, alors* $x \in \{\pm 1, \pm 3, \pm(2+i\sqrt{5}), \pm(2-i\sqrt{5}), \pm 3(2+i\sqrt{5})\}$*. Or* $\pm(2-i\sqrt{5}) \nmid 3(2+i\sqrt{5})$*. En effet, si, par exemple,* $3(2+i\sqrt{5}) = \pm x(2-i\sqrt{5})$*, avec* $x = a + ib\sqrt{5}$*, alors* $a^2 + 5b^2 = 9$ *d'où* $x \in \{\pm 3, \pm(2+i\sqrt{5}), \pm(2-i\sqrt{5})\}$*. Cependant, si* $x = \pm 3$*, alors* $(2+i\sqrt{5}) = \pm(2-i\sqrt{5})$*, si* $x = \pm(2+i\sqrt{5})$*, alors* $3 = \pm(2-i\sqrt{5})$ *et si* $x = \pm(2-i\sqrt{5})$*, alors* $6 + 3i\sqrt{5} = \pm(-1-4i\sqrt{5})$*, ce qui est faux. Donc, les diviseurs de* $3(2+i\sqrt{5})$ *sont* $\pm 1, \pm 3, \pm(2+i\sqrt{5}), \pm 3(2+i\sqrt{5})$*..*

*c) 1/3 et 1/2 +* $i\sqrt{5}$. *Soit* $x = a + ib\sqrt{5} \in \mathbb{Z}[i\sqrt{5}] : x/3$ *et* $x/2 + i\sqrt{5}$. *Les diviseurs de 3 sont* $\pm 1$ *et* $\pm 3$. *Puisque* $\pm 3 \nmid 2 + i\sqrt{5}$, $x = \pm 1/1$ *d'où* 1 *est un pgcd de* 3 *et* $2 + i\sqrt{5}$.

*Supposons que* 3 *et* $2 + i\sqrt{5}$ *admettent un ppcm noté* $m$, *alors* $m/9$ *et* $m/3(2 + i\sqrt{5})$ *(car* $3/9$, $2 + i\sqrt{5}/9$ *et* $3/3(2 + i\sqrt{5})$, $2 + i\sqrt{5}/3(2 + i\sqrt{5})$*). Ainsi, d'après b)* $m = \pm 1$ *ou* $m = \pm 3$ *ou* $m = \pm(2 + i\sqrt{5})$. *Or* $m \neq \pm 1$ *car* $3/m$, $m \neq \pm 3$ *car* $2 + i\sqrt{5}/m$ *et* $m \neq \pm(2 + i\sqrt{5})$ *car* $3/m$.

*Puisque* 3 *et* $2 + i\sqrt{5}$ *n'ont pas de ppcm dans* $\mathbb{Z}[i\sqrt{5}]$, $\mathbb{Z}[i\sqrt{5}]$ *n'est pas principal.*

*d) Supposons que 9 et* $3(2 + i\sqrt{5})$ *admettent un pgcd noté* $d$. *Alors, d'après b),* $d = \pm 1$ *ou* $d = \pm 3$ *ou* $d = \pm(2 + i\sqrt{5})$. *Mais,* $d \neq \pm 1$ *car* $3/d$, $d \neq \pm 3$ *car* $2 + i\sqrt{5}/d$ *et* $d \neq \pm(2 + i\sqrt{5})$ *car* $3/d$.

*D'après 1) et puisque 9 et* $3(2 + i\sqrt{5})$ *n'ont pas de pgcd, alors 9 et* $3(2 + i\sqrt{5})$ *n'ont pas de ppcm.*

*e) Supposons que* $(3, 2 + i\sqrt{5})$ *est principal, i.e.* $\exists x \in \mathbb{Z}[i\sqrt{5}] : (3, 2 + i\sqrt{5}) = (x)$. *D'où,* $x/3$ *et* $x/2 + i\sqrt{5}$ *et d'après c),* $x/\pm 1$ *alors* $(3, 2 + i\sqrt{5}) = \mathbb{Z}[i\sqrt{5}]$. *Ainsi,* $1 = 3(a + ib\sqrt{5}) + (2 + i\sqrt{5})(c + id\sqrt{5})$, *d'où* $1 = 3a + 2c - 5d$ *et* $0 = 3b + 2d + c$. *Alors* $1 = 3(a + b + c - d)$, *ce qui est faux car* $a, b, c, d \in \mathbb{Z}$.

**Exercice 4.3** *On considère l'anneau* $\mathbb{Z}[i] = \{a + ib/a, b \in \mathbb{Z}\}$ *et l'application* $\delta : \mathbb{Z}[i] - \{0\} \longrightarrow \mathbb{N}, x = a + ib \longmapsto \delta(x) = a^2 + b^2$.

*1) Montrer que* $\forall (x, y) \in \mathbb{Z}[i] \times (\mathbb{Z}[i] - \{0\})$, $\exists q, r \in \mathbb{Z}[i]$ *tels que* $x = yq + r$ *avec* $r = 0$ *ou* $\delta(r) < \delta(y)$. *Ainsi,* $\mathbb{Z}[i]$ *est* ***euclidien****. ( On dit qu'un anneau* $A$ *est* ***euclidien*** *si* $A$ *est intègre et s'il existe une application* $\delta : A - \{0\} \longrightarrow \mathbb{N}$ *telle que Pour tout* $(x, y)$ *élément de* $A \times (A - \{0\})$ *il existe* $q, r$ *éléments de* $A$ *tels que* $x = yq + r$ *avec* $r = 0$ *ou* $\delta(r) < \delta(y)$, $q$ *est dit* ***quotient*** *et* $r$ *est dit* ***reste****).*

*2) Montrer que* $\mathbb{Z}[i]$ *est principal.*

**Solution**

*1)* $\forall x = a + ib \in \mathbb{Z}[i], \forall y = c + id \in (\mathbb{Z}[i] - \{0\})$. *On a* $\frac{x}{y} = \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2} = \alpha + i\beta$ *avec* $\alpha, \beta \in \mathbb{Q}$. *Soit* $m$ *(resp.* $n$*) l'entier le plus proche de* $\alpha$ *(resp. de* $\beta$*). i.e.,* $|\alpha - m| \leq \frac{1}{2}$ *et* $|\beta - n| \leq \frac{1}{2}$. *D'où* $x = y(\alpha + i\beta) = y((m + u) + i(n + v)) = y(m + in) + y(u + iv)$ $(u = \alpha - m$ *et* $v = \beta - n)$. *Posons* $q = m + in$ *et* $r = y(u + iv)$. *Alors* $x = yq + r$ *et on a* $q = m + in \in \mathbb{Z}[i]$ *et* $r = x - yq \in \mathbb{Z}[i]$. *On a aussi* $r = 0$ *ou* $\delta(r) = \delta(y(u+iv)) = \delta(y)(u^2+v^2) \leq \delta(y)(\frac{1}{4}+\frac{1}{4}) < \delta(y)$.

*2) Soit* $I$ *un idéal de* $\mathbb{Z}[i]$. *Si* $I = \{0\}$ *alors* $I = (0)$ *est principal. Supposons que* $I \neq \{0\}$. *Soit* $X = \{\delta(x)/x \in I - \{0\}\}$. *On a* $X \neq \emptyset$ *car* $I \neq \{0\}$ *et* $X \subset \mathbb{N}$ *d'où* $X$ *admet un plus petit élément; notons* $\delta(y)$ *cet élément et montrons que* $I = (y)$. *Soit* $x \in I, y \in I - \{0\}$, *alors* $\exists q, r \in \mathbb{Z}[i]$ *tels que* $x = yq + r$, *avec* $r = 0$ *ou* $\delta(r) < \delta(y)$. *Comme* $y, x \in I$, *alors* $r = x - bq \in I$ *d'où* $r = 0$ *sinon* $\delta(r) \in X$ *et* $\delta(r) < \delta(y$, *ce qui contredit la minimalité de* $\delta(y)$ *dans* $X$ *donc* $x = yq \in (y)$ *et ainsi* $I = (y)$ *(on a* $(y) \subset I$ *car* $y \in I$*).*

# Chapitre 5

# Anneaux de Polynômes

**Exercice 5.1**

*1) Soit $P(X) \in \mathbb{Q}[X]$ un polynôme non constant. Montrer que $P'$ divise $P$ si, et seulement si, $P = a(X-\alpha)^n$, où $a, \alpha \in \mathbb{Q}$.*

*2) Soit $P(X) = X^5 - aX^2 - aX + 1 \in \mathbb{Q}[X]$. Déterminer $a$ de manière que $-1$ soit une racine de $P$ d'ordre de multiplicité $\geq 2$.*

*3) Soit $P(X) = 1 + \frac{X}{1} + \frac{X^2}{2!} + ... + \frac{X^n}{n!} \in \mathbb{Q}[X]$. Montrer que $P$ n'a pas de racines multiples.*

**Solution**

*1) Posons $P = a_0 + a_1X + ... + a_nX^n$ avec $a_n \neq 0$. $P' = a_1 + 2a_2X + ... + na_nX^{n-1}$. Supposons que $P'/P$, alors $\exists Q \in \mathbb{Q}[X] : P = P'Q$, d'où $\deg Q = 1$ et le coeffecient dominant de $Q$ est $\frac{1}{n}$, i.e. $Q = \frac{1}{n}X + c$ d'où, en posant $\alpha = -nc$, $nP = (X-\alpha)P'$, i.e., $P = \frac{(X-\alpha)}{n}P'$. Donc $P' = \frac{(X-\alpha)}{n-1}P"$ et par suite $P = \frac{(X-\alpha)^2}{n(n-1)}P"$. Ainsi, on vérifie par récurrence sur $k \in \{1, ..., n\}$ que $P = \frac{(X-\alpha)^k}{n...(n-(k-1))}P^{(k)}$ et alors $P = \frac{(X-\alpha)^n}{n...(n-(n-1))}P^{(n)} = \frac{(X-\alpha)^n}{n!}a_nn! = a_n(X-\alpha)^n$. D'où $nP' = P' + (X-\alpha)P''$ et $(n-1)P' = (X-\alpha)P''$. Aussi, $(n-1)P'' = P'' + (X-\alpha)P'''$ alors $(n-2)P'' = (X-\alpha)P'''$ ainsi, $P = \frac{(X-\alpha)^n}{n!}P^{(n)} = a(X-\alpha)^n$. D'autre part, si $P = a(X-\alpha)^n$, alors $P' = na(X-\alpha)^{n-1}/P$.*

*2) $-1$ est une racine de $P$ d'ordre de multiplicité $\geq 2$ si, et seulement si, $(X+1)^2/P$ si, et seulement si, $P(-1) = P'(-1) = 0$ si, et seulement si, $a = -5$.*

*3) Supposons que $\alpha$ est une racine multiple de $P$, alors $P(\alpha) = P'(\alpha) = 0$. Or, $P' = 1 + \frac{X}{1} + ... + \frac{X^{n-1}}{(n-1)!} = P - \frac{X^n}{n!}$ et ainsi $P'(\alpha) = P(\alpha) - \frac{\alpha^n}{n!} = -\frac{\alpha^n}{n!} = 0$ d'où $\alpha = 0$. Cependant, $\alpha = 0$ n'est pas une racine de $P$.*

**Exercice 5.2** *Soit $P = a_0 + a_1X + ... + a_nX^n \in \mathbb{Z}[X]$. On suppose que $\alpha = \frac{p}{q} \in \mathbb{Q}$ est une racine de $P$ avec $(p,q) \in \mathbb{Z} \times \mathbb{Z}^*$ et $p \wedge q = 1$.*

*1) Montrer que $p/a_0$, $q/a_n$ et en déduire que si $a_n = 1$, alors $\alpha \in \mathbb{Z}$.*

*2) Montrer que $\forall m \in \mathbb{Z}$, $p - mq/\tilde{P}(m)$ et en déduire que $p - q/\tilde{P}(1)$ et que $p + q/\tilde{P}(-1)$.*

*3) Application :*

*a) Déterminer les racines rationnelles du polynôme $P = X^3 - 6X^2 + 15X - 14 \in \mathbb{Z}[X]$.*

*b) Soit $P \in \mathbb{Z}[X]$. Montrer que si $\tilde{P}(0)$ et $\tilde{P}(1)$ sont des entiers impairs, alors $P$ n'a pas de racines dans $\mathbb{Z}$.*

**Solution**

*1) On a* $a_0 + a_1\frac{p}{q} + ... + a_n\frac{p^n}{q^n} = 0$ *d'où* $a_0q^n + a_1pq^{n-1} + ... + a_{n-1}qp^{n-1} + a_np^n = 0$ *et* $-p(a_1q^{n-1} + ... + a_{n-1}qp^{n-2} + a_np^{n-1}) = a_0q^n$ *et ainsi* $p/a_0q^n$. *Puisque* $p \wedge q = 1$, $p/a_0$. *De même, on montre que* $q/a_n$.

*En particulier, si* $a_n = 1$, *i.e., si* $P$ *est unitaire,* $q/1$ *alors* $q = \pm 1$ *et par conséquent* $\alpha = \frac{p}{q} \in \mathbb{Z}$.

*2) On a* $P = \sum_{k=0}^{n} a_kX^k \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$. *Alors, d'après la formule de Taylor, on a* $P = \sum_{k=0}^{n} \frac{P^{(k)}(m)}{k!}(X-m)^k$. *En posant* $c_k = \frac{P^{(k)}(m)}{k!} \in \mathbb{Q}$, $P = c_0 + c_1(X-m) + ... + c_n(X-m)^n$. *D'où* $c_n = a_n \in \mathbb{Z}$, $c_{n-1} - c_n.C_n^1.m = a_{n-1}$ *et donc* $c_{n-1} = c_n.C_n^1.m + a_{n-1} \in \mathbb{Z}$ *et ainsi on vérifie aussi que* $c_{n-2}, ..., c_1, c_0 \in \mathbb{Z}$. *Puisque* $P(\frac{p}{q}) = 0$, $c_0q^n = -c_1(p-mq)q^{n-1} - ... - c_n(p-mq)^n$ *d'où* $(p-mq)/c_0q^n$ *et par conséquent* $(p-mq)/c_0 = P(m)$ *car* $(p-mq) \wedge q^n = 1$ $(p \wedge q = 1)$.

*En prenant* $m = 1$ *puis* $m = -1$, *on a* $(p-q)/P(1)$ *et* $p+q/P(-1)$.

<u>*Autre méthode :*</u> *Puisque* $\frac{p}{q}$ *est une racine de P,* $\exists Q \in \mathbb{Q}[X] : P = (X - \frac{p}{q})Q$ *d'où* $qP = (qX-p)Q$. *Posons* $Q = \sum_{i=0}^{l} \frac{b_i}{c_i}X^i$, *avec* $(b_i, c_i) \in \mathbb{Z} \times \mathbb{Z}^*$, *et* $m = ppcm(c_1, ..., c_l)$, *on a* $mQ = Q_1 \in \mathbb{Z}[X]$ *et en posant,* $Q_1 = dQ_2$, *où* $d = c(Q_1)$, *on a* $Q_2 \in \mathbb{Z}[X]$ *est primitif. Comme,* $qmP = (qX-p)dQ_2$, $c(mqP) = c((qX-p)dQ_2)$ *d'où* $mqc(P) = dc(qX-p)c(Q_2)$. *Ainsi,* $mqc(P) = d$, *car* $c(qX-p) = p \wedge q = 1$ *et* $Q_2$ *est primitif, et donc* $qmP = (qX-p)mqc(P)Q_2$. *Puisque* $\mathbb{Z}$ *est intègre et* $qm \neq 0$, *alors* $P = (qX-p)c(P)Q_2$ *et ainsi* $(qm-P)/P(m)$ *dans* $\mathbb{Z}$.

*On a , d'après 1, si* $m = 0$, *alors* $p/a_0$.

*3)*

*a) Supposons que* $\alpha = \frac{p}{q} \in \mathbb{Q}$ *est une racine de P. Alors, d'après 1)* $\alpha = \frac{p}{q} \in \mathbb{Z}$ *car P est unitaire et ainsi on peut supposer que* $q = 1$. *On a aussi* $p/a_0 = -14$ *d'où* $p \in \{\pm 1, \pm 2, \pm 7, \pm 14\}$. *D'autre part, on a* $p - q = p - 1/P(1) = -4$ *d'où* $p \notin \{1, -2, \pm 7, \pm 14\}$ *et ainsi les valeurs possibles de p sont -1 et 2. Puisque* $P(-1) = -6$ *et* $P(2) = 0$, *P admet une seule racine rationnelle* $\alpha = 2$.

*b) On a* $p/a_0 = P(0)$, $p - q/P(1)$ *et puisque* $P(0)$ *et* $P(1)$ *sont impairs, p et* $p-q$ *sont impairs et par conséquent* $q = p - (p-q)$ *est pair d'où* $q \neq 1$.

**Exercice 5.3** *Soit A un anneau commutatif unitaire. Montrer que* $A[X]$ *est un anneau principal si, et seulement si, A est un corps.*

**Solution**

*On a, d'après le cours, si A est un corps, alors* $A[X]$ *est un anneau principal. Réciproquement, soit* $a \in A - \{0\}$. *Puisque* $A[X]$ *est principal, l'idéal* $(a, X)$ *est principal, i.e.* $\exists P \in A[X] : (a, X) = (P)$ *d'où* $P/a$ *et* $P/X$. *Alors,* $P = b \in A$ *car* $P/a$ *et* $P = b \in \mathcal{U}(A)$ *car* $P/X$ *d'où* $(a, X) = (P) = A$ *alors* $\exists Q, S \in A[X] : 1 = aQ + XS$. *Ainsi* $1 = aQ(0)$ *et donc a est inversible.*

**Exercice 5.4**

*1) Dans* $\mathbb{Q}[X]$, *trouver une expression plus simple des idéaux suivants :*

*a)* $2X\mathbb{Q}[X] + (X+1)\mathbb{Q}[X]$.

*b)* $2X\mathbb{Q}[X] \cap (X+1)\mathbb{Q}[X]$.

*c)* $2X\mathbb{Q}[X].(X+1)\mathbb{Q}[X]$.

*2) Déterminer un pgcd des polynômes $P = X^4 + 1$ et $Q = X^3 + X + 1$ dans $\mathbb{Z}/2\mathbb{Z}[X]$ et dans $\mathbb{Z}/3\mathbb{Z}[X]$.*

*Dans le cas où $P$ et $Q$ sont premiers entre eux, trouver deux polynômes $U$ et $V$ tels que $UP + VQ = \bar{1}$.*

**Solution**

*1) Puique $\mathbb{Q}[X]$ est un anneau principal, $(P) + (Q) = (P \wedge Q)$ et $(P) \cap (Q) = (P \vee Q)$. Alors,*

*a)* $(2X) + (X + 1) = (2X \wedge (X + 1)) = (1) = \mathbb{Q}[X]$.

*b)* $(2X) \cap (X + 1) = (2X \vee (X + 1)) = (2X(X + 1))$

*c)* $(2X).(X + 1) = (2X(X + 1))$ *(cf. exercice 3.2).*

*2) Dans $\mathbb{Z}/2\mathbb{Z}[X]$ : $P = QQ_1 + R_1$ avec $Q_1 = X, R_1 = X^2 + X + \bar{1}$ ; $Q = R_1Q_2 + R_2$ avec $Q_2 = X + \bar{1}, R_2 = X$ ; $R_1 = R_2Q_3 + R_3$ avec $Q_3 = X + \bar{1}$ et $R_3 = \bar{1}$. Ainsi, $P \wedge Q = \bar{1}$. D'autre part, on a $\bar{1} = R_3 = R_1 - R_2Q_3 = (P - QQ_1) - (Q - (P - QQ_1)Q_2)Q_3 = P(1 + Q_2Q_3) + Q(-Q_1 - Q_1Q_2Q_3 - Q_3)$ ,i.e., $X^2P + (X^3 + X + \bar{1})Q = \bar{1}$.*

*Dans $\mathbb{Z}/3\mathbb{Z}[X]$, $P = QQ_1 + R_1$ avec $Q_1 = X, R_1 = \bar{2}X^2 + \bar{2}X + \bar{1}$ et $Q = R_1Q_2 + R_2$ avec $Q_2 = \bar{2}X + \bar{1}, R_2 = \bar{0}$. Alors, $P \wedge Q = R_1 = \bar{2}X^2 + \bar{2}X + \bar{1}$.*

**Exercice 5.5**

*1) Soit $K$ un corps (commutatif). Montrer que $K[X]/(X) \simeq K$. L'idéal $(X)$ est-il premier ? maximal ?*

*2) Dans $\mathbb{Z}[X]$, l'idéal $(X)$ est-il premier ? maximal ?. En déduire que $\mathbb{Z}[X]$ n'est pas principal.*

*3) Montrer que $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$. Dans $\mathbb{R}[X]$, l'idéal $(X^2+1)$ est-il premier ? maximal ?*

**Solution**

*1) On considère l'application $f : K[X] \longrightarrow K, P \longmapsto P(0)$. On vérifie facilement que f est un homomorphisme d'anneaux surjectif et que kerf=(X). Alors, en appliquant le premier théorème d'isomorphisme, on a $K[X]/(X) \simeq K$ et puisque $K$ est un corps, $(X)$ est maximal (alors premier).*

*2) De même que 1), on a $\mathbb{Z}[X]/(X) \simeq \mathbb{Z}$, d'où $(X)$ est premier car $\mathbb{Z}$ est intègre. mais, $(X)$ n'est pas maximal car $\mathbb{Z}$ n'est pas un corps. Puisque $(X)$ est un idéal premier non nul et $(X)$ n'est pas maximal, $\mathbb{Z}[X]$ n'est pas principal car dans un anneau principal, tout idéal premier non nul est maximal.*

*3) On considère l'application $f : \mathbb{R}[X] \longrightarrow \mathbb{C}, P \longmapsto P(i)$. il est évident que $f$ est un homomorphisme d'anneaux surjectif. On a aussi $\ker f = (X^2 + 1)$. en effet, $(X^2 + 1) \subset \ker f$ car $X^2+1 \in \ker f$. Pour montrer l'autre inclusion, on utilise l'une des deux méthode suivantes :*

*<u>1ère Méthode :</u> Soit $P \in \ker f$, alors $P(i) = 0$ et puisque $P \in \mathbb{R}[X]$, $P(-i) = 0$ d'où, comme $\mathbb{C}$ est intègre, $(X - i)(X + i)/P$ dans $\mathbb{C}[X]$, i.e., $P = (X^2 + 1)Q$ avec $Q \in \mathbb{C}[X]$. Posons $P = \sum_{k=0}^{n} a_kX^k$ avec $a_n \neq 0$ (le cas où $P = 0$ est trivial), alors $Q = \sum_{k=0}^{n-2} b_kX^k$ et par identification, on vérifie que $Q = \sum_{k=0}^{n-2} b_kX^k \in \mathbb{R}[X]$ et donc $P \in (X^2 + 1)$.*

*<u>2ème Méthode</u> : Soit $P \in \ker f$. En effectuant la division euclidienne de $P$ par $X^2 + 1$, on obtient $P = (X^2 + 1)Q + R$ avec $Q, R \in \mathbb{R}[X]$ et degR $< 2$ d'où $R = aX + b$ avec $a, b \in \mathbb{R}$. D'autre part, on a $0 = f(P) = P(i) = ai + b$ d'où $a = b = 0$, $R = 0$ et ainsi $P \in (X^2 + 1)$.*

*En utilisant le premier théorème d'isomorphisme, on a* $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ *d'où* $(X^2+1)$ *est maximal car* $\mathbb{C}$ *est un corps. Puisque* $(X^2+1)$ *est un idéal maximal,* $(X^2+1)$ *est un idéal premier.*

**Exercice 5.6** *Soient* $A$ *un anneau intègre et* $P(X) \in A[X]$*. Montrer que si* $S(X) = P(X+c)$*, où* $c \in A$*, est irréductible dans* $A[X]$*, alors* $P(X)$ *est irréductible dans* $A[X]$*.*

*Application : Soit* $P(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}[X]$*. Montrer que* $P$ *est irréductible dans* $\mathbb{Q}[X]$*.*

**Solution**

*Puisque* $S(X) \neq 0$ *et* $S(X) \notin \mathcal{U}(A[X]) = \mathcal{U}(A)$, $P(X) \neq 0$ *et* $P(X) \notin \mathcal{U}(A[X]) = \mathcal{U}(A)$*. Soit* $Q(X) \in A[X] : Q(X)/P(X)$ *alors* $\exists T(X) \in A[X] : P(X) = Q(X)T(X)$ *d'où* $S(X) = P(X+c) = Q(X+c)T(X+c)$ *ainsi* $Q(X+c) \in \mathcal{U}(A)$ *ou* $T(X+c) \in \mathcal{U}(A)$ *et par conséquent* $Q(X) \in \mathcal{U}(A)$ *ou* $T(X) \in \mathcal{U}(A)$*.*

*Application : Soit* $S(X) = P(X+1)$*, on a* $S(X) = X^4 + 5X^3 + 10X^2 + 10X + 5 \in \mathbb{Z}[X]$*. En prenant* $p = 5$*, on a* $p/a_0 = 5$, $p/a_1 = 10$, $p/a_2 = 10$, $p/a_3 = 5$, $p \nmid a_4 = 1$ *et* $p^2 \nmid a_0 = 5$*. Comme* $\mathbb{Z}$ *est principal et* $S$ *est primitif, alors, d'après le critère d'Eisenstein,* $S(X)$ *est irréductible dans* $\mathbb{Z}[X]$ *et d'après la question précédente,* $P(X)$ *est irréductible dans* $\mathbb{Z}[X]$*. Ainsi, d'après le cours,* $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$*.*

**Exercice 5.7**

*1) Déterminer tous les polynômes irréductibles de degrés 2, 3 et 4 à coefficients dans* $\mathbb{Z}/2\mathbb{Z}$*.*

*2) Décomposer les polynômes suivants en produit de polynômes irréductibles dans* $\mathbb{Z}/3\mathbb{Z}[X]$ *:*

*a)* $X^3 + X + \bar{2}$*.*

*b)* $X^4 + X^3 + X + \bar{1}$*.*

**Solution**

*1) * Polynômes irréductibles de degré 2 dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *: soit* $P = \overline{a}X^2 + \overline{b}X + \overline{c} \in \mathbb{Z}/2\mathbb{Z}[X]$ *de degré 2 d'où* $\overline{a} = \bar{1}$*, i.e.,* $P = X^2 + \overline{b}X + \overline{c}$*. Puisque* $P$ *est de degré 2 et* $\mathbb{Z}/2\mathbb{Z}$ *est un corps,* $P$ *est irréductible si, et seulement si,* $P$ *n'a pas de racines dans* $\mathbb{Z}/2\mathbb{Z}$*, i.e.,* $\overline{c} \neq \bar{0}$ *et* $\overline{b} + \overline{c} \neq \bar{1}$*, i.e.,* $\overline{c} = \bar{1}$ *et* $\overline{b} = \bar{1}$ *et ainsi le seul polynôme irréductible de degré 2 dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *est le polynôme* $P = X^2 + X + \bar{1}$*.*

** Polynômes irréductibles de degré 3 dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *: soit* $P = \overline{a}X^3 + \overline{b}X^2 + \overline{c}X + \overline{d} \in \mathbb{Z}/2\mathbb{Z}[X]$ *de degré 3 d'où* $\overline{a} = \bar{1}$*, i.e.,* $P = X^3 + \overline{b}X^2 + \overline{c}X + \overline{d}$*. Puisque* $P$ *est de degré 3 et* $\mathbb{Z}/2\mathbb{Z}$ *est un corps,* $P$ *est irréductible si, et seulement si,* $P$ *n'a pas de racines dans* $\mathbb{Z}/2\mathbb{Z}$*, i.e.,* $\overline{d} \neq \bar{0}$ *et* $\overline{b} + \overline{c} + \overline{d} \neq \bar{1}$*, i.e.,* $\overline{d} = \bar{1}$ *et* $\overline{b} + \overline{c} = \bar{1}$ *et ainsi les seuls polynômes irréductibles de degré 3 dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *sont les polynômes* $P_1 = X^3 + X^2 + \bar{1}$ *et* $P_2 = X^3 + X + \bar{1}$*.*

** Polynômes irréductibles de degré 4 dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *: soit* $P = \overline{a}X^4 + \overline{b}X^3 + \overline{c}X^2 + \overline{d}X + \overline{e} \in \mathbb{Z}/2\mathbb{Z}[X]$ *de degré 4, alors* $\overline{a} = \bar{1}$*, i.e.,* $P = X^4 + \overline{b}X^3 + \overline{c}X^2 + \overline{d}X + \overline{e}$*. Puisque* $\mathbb{Z}/2\mathbb{Z}$ *est un corps et* $P$ *est de degré 4,* $P$ *est réductible si, et seulement si,* $\exists Q \in \mathbb{Z}/2\mathbb{Z}[X]$ *de degré 1 ou 2 ou 3 tel que* $Q/P$*. i.e.,* $P$ *a une racine dans* $\mathbb{Z}/2\mathbb{Z}$ *ou* $P$ *est le produit de deux polynômes irréductibles de degrés 2. Alors,* $P$ *est irréductible si ,et seulement si,* $\overline{e} = 1$ *et* $\overline{b} + \overline{c} + \overline{d} = 1$ *et* $P \neq (X^2 + X + \bar{1})^2 = X^4 + X^2 + \bar{1}$ *(d'après la première question, le seul polynôme irrédictibles de degré 2 dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *est le polynôme* $X^2 + X + \bar{1}$*) et ainsi les polynômes de degrés 4 irréductibles dans* $\mathbb{Z}/2\mathbb{Z}[X]$ *sont :* $X^4 + X^3 + \bar{1}$, $X^4 + X + \bar{1}$ *et* $X^4 + X^3 + X^2 + X + \bar{1}$*.*

*2)* $X^3 + X + \bar{2} = (X + \bar{1})(X^2 + \bar{2}X + \bar{2})$ *et* $X^4 + X^3 + X + \bar{1} = (X + \bar{1})^4$*.*

**Exercice 5.8** *Montrer en utilisant le critère d'Eisenstein ou la réduction modulo p que les polynômes suivants sont irréductibles.*

*1)* $X^5 - 12X^3 + 36X - 12 \in \mathbb{Z}[X]$.

*2)* $6X^3 + 10X^2 + 8X + 2 \in \mathbb{Q}[X]$

*3)* $X^3 + Y^3 + 1 \in \mathbb{C}[X, Y]$

*4)* $X^2 + Y^6 + 7Y^4 + XY^3 + 2X^2Y^2 + 5Y + X + 1 \in \mathbb{Q}[X, Y]$.

**Solution**

*1) On prend* $p = 3$ *et on utilise le critère d'Eisenstein.*

*2) Posons* $P = 2Q$, *où* $Q = 3X^3 + 5X^2 + 4X + 1 \in \mathbb{Q}[X]$. *Puisque P et Q sont associés dans* $\mathbb{Q}[X]$, *il suffit de vérifier que Q est irréductible dans* $\mathbb{Q}[X]$.

*On a* $Q \in \mathbb{Z}[X]$ *et Q est primitif. En prenant p=2 et en calculant la réduction modulo 2 de Q, on obtient* $\varphi(Q) = X^3 + X^2 + \bar{1} \in (\mathbb{Z}/2\mathbb{Z})[X]$.

*Comme* $\varphi(Q) = X^3 + X^2 + \bar{1}$ *n'a pas de racines dans* $(\mathbb{Z}/2\mathbb{Z})$, $\varphi(Q)$ *est irréductible dans* $(\mathbb{Z}/2\mathbb{Z})[X]$ *et par suite Q est irréductible dans* $\mathbb{Z}[X]$. *Ainsi, Q est irréductible dans* $\mathbb{Q}[X]$ *et donc P est irréductible dans* $\mathbb{Q}[X]$.

*3) On pose* $X^3 + Y^3 + 1 = Y^3 + (X^3 + 1)$ *et on considère* $X^3 + Y^3 + 1$ *comme un polynôme à une indéterminée Y et à cofficients dans l'anneau principal* $A = \mathbb{C}[X]$. *On prend* $p = X + 1$ *et on applique le critère d'Eisenstein au polynôme* $P(Y) = X^3 + Y^3 + 1 = Y^3 + (X^3 + 1)$.

*4) On pose* $X^2 + Y^6 + 7Y^4 + XY^3 + 2X^2Y^2 + 5Y + X + 1 = (1 + 2Y^2)X^2 + (Y^3 + 1)X + (Y^6 + 7Y^4 + 5Y + 1)$ *et on considère* $X^2 + Y^6 + 7Y^4 + XY^3 + 2X^2Y^2 + 5Y + X + 1 = P(X)$ *comme un polynôme à une indéterminée X et à cofficients dans l'anneau principal* $A = \mathbb{Q}[Y]$.

*Le polynôme* $P(X)$ *est primitif. En effet, posons* $D = c(P(X))$ *alors* $D/1 + 2Y^2$ *dans A et puisque* $1 + 2Y^2$ *est irréductible dans A, D est inversible ou* $D \sim 1 + 2Y^2$. *Supposons que* $D \sim 1 + 2Y^2$, *alors* $1 + 2Y^2/Y^3 + 1$, *ce qui est faux et donc* $D = 1$.

*On prend* $p = Y$ *et on applique la réduction modulo p au polynôme* $P(X)$, *on obtient* $\varphi(P) = X^2 + X + 1 \in A[X]/(Y) = \mathbb{Q}[X, Y]/(Y) \simeq \mathbb{Q}[X]$. *Puique* $\varphi(P)$ *est irréductible dans* $\mathbb{Q}[X]$ *car* $X^2 + X + 1$ *n'a pas de racines dans* $\mathbb{Q}, P$ *est irréductible dans* $A[X] = \mathbb{Q}[X, Y]$.

**Exercice 5.9**

*1) Soient K un corps (commutatif), a et b deux éléments de K. Quels sont parmis les idéaux suivants ceux qui sont premiers et ceux qui sont maximaux.*

*a) L'idéal* $(X - a)$ *de* $K[X]$.

*b) L'idéal* $(Y - b)$ *de* $K[X, Y]$.

*c) L'idéal* $(X - a, Y - b)$ *de* $K[X, Y]$.

*2) Les idéaux* $(X^2 + 1)$ *et* $(X^2 - 1)$ *de l'anneau* $\mathbb{Q}[X, Y]$ *sont-ils premiers ? maximaux ?*

**Solution**

*1)*

*a) On considère l'homomorphisme d'anneaux* $f : K[X] \longrightarrow K, P(X) \longmapsto \widetilde{P}(a)$. *On a f est surjectif et* $\ker f = (X - a)$. *Ainsi,* $K[X]/(X - a) \simeq K$ *d'où* $(X - a)$ *est un idéal maximal et donc premier.*

*b) On pose* $A = K[X]$ *et on considère l'homomorphisme d'anneaux* $f : A[Y] \longrightarrow A$, $P(Y) \longmapsto P(b)$. *On a f est surjectif et* $\ker f = (Y - b)$. *Ainsi,* $A/(Y - b) \simeq A$ *d'où* $(Y - b)$ *est un idéal premier car A est intègre et* $(Y - b)$ *n'est pas maximal car A n'est pas un corps.*

*c) On considère l'homomorphisme d'anneaux* $f : K[X, Y] \longrightarrow K, P(X, Y) \longmapsto P(a, b)$. *On a f est surjectif. Montrons que* $ker f = (X - a, Y - b)$. *Puisque* $(X - a, Y - b) \subset \ker f$, *il*

*suffit de vérifier que* $\ker f \subset (X-a, Y-b)$ *: soit* $P(X,Y) \in \ker f$*. En posant* $A = K[X]$, $P(X,Y) = Q(Y) \in A[Y]$ *et en effectuant la division euclidienne de* $Q(Y)$ *par* $Y-b$*, on obtient* $Q(Y) = (Y-b)S(Y) + R(Y)$ *avec* $S(Y), R(Y) \in A[Y]$ *et* $\deg_Y R(Y) < 1$*, i.e.* $R(Y) \in A$*, i.e.* $R(Y) = T(X) \in A = K[X]$ *est un polynôme à une seule indéterminée* $X$ *et à coefficients dans* $K$.

*Ainsi,* $P(a,b) = T(a) = 0$ *d'où* $R = (X-a)U(X)$*, avec* $U(X) \in K[X]$*, alors* $P(X,Y) = (Y-b)S(Y) + (X-a)U(X) \in (X-a, Y-b)$.

*2) On considère l'homomorphisme d'anneaux* $f : \mathbb{Q}[X,Y] \longrightarrow \mathbb{C}[Y], P(X,Y) \longmapsto P(i,Y)$*. On a* $\ker f = (X^2+1)$*. En effet, puisque,* $(X^2+1) \subset \ker f$*, il suffit de vérifier que* $\ker f \subset (X^2+1)$.

*Soit* $P \in \ker f$*, en considérant* $P(X,Y) = Q(X)$ *comme un polynôme à une indéterminée* $X$ *et à coefficients dans* $A = \mathbb{Q}[Y]$ *et en effectuant la division euclidienne de* $P$ *par* $X^2+1$*, on obtient* $P = (X^2+1)Q + R$ *avec* $Q, R \in A[X]$ *et* $\deg_X R < 2$ *d'où* $R = aX + b$ *avec* $a, b \in A{=}\mathbb{Q}[Y]$*. D'autre part, on a* $0 = f(P) = P(i) = ai + b$ *d'où* $a = b = 0$*,* $R = 0$ *et ainsi* $P \in (X^2+1)$.

*Aussi, on a* $\operatorname{Im} f = (\mathbb{Q}[i])[Y]$*. En effet, soit* $P(X,Y) = \sum_{j+k=0}^{n} a_{jk} X^j Y^k \in \mathbb{Q}[X,Y]$*,* $f(P) = \sum_{j+k=0}^{n} a_{jk} i^j Y^k$ *et puisque* $a_{jk} i^j \in Q[i]$*,* $f(P) \in (\mathbb{Q}[i])[Y]$*. Inversement, soit* $P(Y) = \sum_{k=0}^{n} \alpha_k Y^k \in (\mathbb{Q}[i])[Y]$*, i.e.,* $\alpha_k = a_k + ib_k$*, où* $a_k, b_k \in \mathbb{Q}$*. D'où* $P(Y) = \sum_{k=0}^{n} a_k Y^k + \sum_{k=0}^{n} ib_k Y^k = f(\sum_{k=0}^{n} a_k Y^k + \sum_{k=0}^{n} b_k X Y^k) \in \operatorname{Im} f$.

*Ainsi,* $\mathbb{Q}[X,Y]/(X^2+1) \simeq (\mathbb{Q}[i])[Y]$ *d'où* $(X^2+1)$ *est un idéal premier car* $(\mathbb{Q}[i])[Y]$ *est intègre et* $(X^2+1)$ *n'est pas maximal car* $(\mathbb{Q}[i])[Y]$ *n'est pas un corps.*

*L'idéal* $(X^2-1)$ *n'est pas premier car* $(X-1)(X+1) \in (X^2-1)$ *mais* $X-1 \notin (X^2-1)$ *et* $X+1 \notin (X^2-1)$.

*On peut aussi remarquer que puisque* $X^2-1$ *n'est pas irréductible dans* $\mathbb{Q}[X,Y]$*,* $X^2-1$ *n'est pas premier dans* $\mathbb{Q}[X,Y]$.

**Exercice 5.10** *On considère l'homomorphisme d'anneaux* $\varphi : \mathbb{C}[X,Y] \longrightarrow \mathbb{C}[X]$, $P(X,Y) \longmapsto P(X, X^2)$.

*1) Montrer que* $\ker \varphi = (Y - X^2)$.

*2) En déduire que l'anneau* $\mathbb{C}[X,Y]/(Y-X^2)$ *est un anneau principal.*

**Solution**

*1) On a* $(Y-X^2) \subset \ker \varphi$*. Pour l'autre inclusion, soit* $P(X,Y) \in \ker \varphi$*. En considérant* $P(X,Y) = Q(Y) \in A[Y]$ *comme un polynôme à une indéterminée* $Y$ *et à coefficients dans* $A$*, où* $A = \mathbb{C}[X]$*, et en effectuant la division euclidienne de* $Q$ *par* $Y - X^2$*, on obtient* $P(X,Y) = Q(Y) = (Y-X^2)S(Y) + R(Y)$*, avec* $S(Y), R(Y) \in A[Y]$ *et* $\deg_Y R < 1$*, i.e.* $R = T(X) \in A$*. Comme* $\varphi(P) = 0$*,* $\varphi(R) = R = 0$ *et ainsi* $P(X,Y) = (Y-X^2)S(Y)$.

*2) Puisque* $\varphi$ *est un homomorphisme d'anneaux surjectif et* $\ker\varphi = (Y-X^2)$*, on a* $\mathbb{C}[X,Y]/((Y-X^2) \simeq \mathbb{C}[X]$ *et par suite* $\mathbb{C}[X,Y]/((Y-X^2)$ *est un anneau principal.*

**Exercice 5.11** *Factoriser les polynômes suivants :*

*1)* $X^2 + Y^2 + Z^2 - XY - XZ - YZ$ *dans* $\mathbb{C}[X, Y]$.

*2)* $X^3 + Y^3 + Z^3 - 3XYZ$ *dans* $\mathbb{Z}[X, Y, Z]$.

**Solution**

*1) On cherche* $Q \in \mathbb{C}[X, Y, Z] : \deg Q = 1$ *et* $Q/P = X^2 + Y^2 + Z^2 - XY - XZ - YZ$. *Alors* $\exists S \in \mathbb{C}[X, Y, Z] : P = QS$. *Puisque* $P$ *est homogène et* $\mathbb{C}$ *est intègre,* $Q$ *et* $S$ *sont homogènes. Comme* $degP = 2$ *et* $degQ = 1$, $degS = 1$. *Posons* $Q = aX + bY + cZ$ *et* $S = a'X + b'Y + c'Z$, *avec* $a, b, c, a', b', c' \in \mathbb{C}$. *Ainsi, puisque* $P = QS$, $aa' = 1, bb' = 1, cc' = 1, ab' + ba' = -1, ac' + a'c = -1, bc' + b'c = -1$. *Si* $a = a' = 1$, $b + \frac{1}{b} = -1$ *et on prend* $b = j$ ($j = e^{i\frac{2\pi}{3}}$) *d'où* $b' = j^2$. *On a aussi* $c + \frac{1}{c} = -1$ *et comme* $jc' + j^2c = -1$, *on prend* $c = j^2$ *et par suite* $c' = j$. *Donc* $P = (X + jY + j^2Z)(X + j^2Y + jZ)$ *et pusique* $\deg Q = \deg S = 1$ *et* $\mathbb{C}$ *est un corps,* $Q$ *et* $S$ *sont irréductibles.*

*2)* $X^3 + Y^3 + Z^3 - 3XYZ = (X + Y + Z)(X^2 + Y^2 + Z^2 - XY - XZ - YZ)$.

**Exercice 5.12** *On considère l'anneau* $A = \mathbb{Z}[i\sqrt{3}] = \{a + ib\sqrt{3}/\ a, b \in \mathbb{Z}\}$

*1) Déterminer* $\mathcal{U}(A)$

*2) Déterminer le corps de fractions* $K$ *de l'anneau* $A$.

*3) Montrer que le polynôme* $X^2 - X + 1$ *est irréductible dans* $A[X]$.

*4) le polynôme* $X^2 - X + 1$ *est-il irréductible dans* $K[X]$ ?

*5) Conclure.*

**Solution**

*1) On a* $\mathcal{U}(A) = \{-1, 1\}$.

*2) On vérifie facilement que* $Fr(A) = \mathbb{Q}[i\sqrt{3}]$.

*3) Posons* $P(X) = X^2 - X + 1$. *On a* $P(X) \neq 0$ *et* $P(X) \notin \mathcal{U}(A[X]) = \mathcal{U}(A) = \{-1, 1\}$. *Soit* $Q(X) \in A[X] : Q(X)/P(X)$, *alors* $\exists S(X) \in A[X] : P(X) = Q(X).S(X)$ *d'où* $2 = degQ(X) + degS(X)$ *ainsi* $degQ(X) \in \{0, 1, 2\}$.

*Or,* $\deg Q(X) \neq 1$. *En effet, si* $degQ(X) = 1$, *i.e.,* $Q(X) = aX + b$, *où* $a \in A - \{0\}, b \in A$, *alors* $S(X) = a'X + b'$, *avec* $a' \in A - \{0\}, b' \in A$ *et ainsi* $a \in \mathcal{U}(A) = \{-1, 1\}$ *car* $P(X) = Q(X)S(X)$ *et* $P(X)$ *est unitaire. Par conséquent,* $P(X)$ *a une racine dans* $A$, *ce qui est faux.*

*Si* $degQ(X) = 0$, *alors* $Q(X) = a \in A$ *et* $S(X) = a'X^2 + b'X + c'$ *et par suite* $aa' = 1$, *i.e.,* $Q(X) \in \mathcal{U}(A[X])$. *Dans le cas où* $degQ(X) = 2$, *on a* $S(X) = a \in A$ *et* $Q(X) = a'X^2 + b'X + c'$ *et par suite* $aa' = 1$, *i.e.,* $S(X) \in \mathcal{U}(A[X])$.

*4) Le polynôme* $X^2 - X + 1$ *n'est pas irréductible dans* $K[X]$ *car* $X^2 - X + 1$ *a une racine dans* $K$. *(les deux racines de* $X^2 - X + 1$ *sont* $-\overline{j} = \frac{1+i\sqrt{3}}{2}$ *et* $-j = \frac{1-i\sqrt{3}}{2}$ *et on a* $-\overline{j}, -j \in K$).

*5) Puisque le polynôme P est non constant et est irréductible dans A[X] mais, P n'est pas irréductible dans K[X], où* $K = Fr(A)$, *alors A n'est pas un anneau principal.*

**Exercice 5.13** *Soit* $P = X^3 - 2X^2 + 4X + 2 \in \mathbb{Q}[X]$.

*1) Montrer que* $\mathbb{Q}[X]/(P)$ *est un corps.*

*2) On considère la surjection canonique* $s : \mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]/(P)$ *et on note* $y = s(X^2) = \overline{X^2}$. *Dire pourquoi* $y$ *est inversible et calculer l'inverse de* $y$ *dans* $\mathbb{Q}[X]/(P)$.

**Solution**

*1) Le polynôme* $P$ *est irréductible dans* $Z[X]$. *En effet, on remarque que* $P$ *est primitif, non constant ; on prend* $p = 2$ *et on utilise le critère d'Eisenstein.*

*Puisque $\mathbb{Z}$ est principal, $\mathbb{Q} = Fr(\mathbb{Z})$ et $P$ est un polynôme non constant et irréductible dans $\mathbb{Z}[X]$, alors $P$ est irréductible dans $\mathbb{Q}[X]$ et par suite l'idéal $(P)$ est un idéal maximal de $\mathbb{Q}[X]$ car $\mathbb{Q}[X]$ est un anneau principal. Ainsi, $\mathbb{Q}[X]/(P)$ est un corps.*

*2) On a $X^2 \notin (P)$ car si $X^2 = PQ$, où $Q \in \mathbb{Q}[X]$, alors 2=3+degQ, ce qui est faux. Ainsi, $y = s(X^2) = \overline{X^2} \neq \overline{0}$ et donc $y$ est inversible dans le corps $\mathbb{Q}[X]/(P)$.*

*Puisque $P$ est irréductible dans Q[X] et $P$ et $X^2$ ne sont pas associés, $P$ et $X^2$ sont premiers entre eux dans l'anneau principal Q[X]. Ainsi, $\exists U(X), V(X) \in Q[X] : X^2U(X) + P(X)V(X) = 1$. En utilisant l'algorithme d'Euclide, on vérifie que si $U(X) = X^2 - \frac{5}{2}X + 5$ et $V(X) = -X + \frac{1}{2}$, alors $X^2U(X) + P(X)V(X) = 1$. En passant au classes modulo P, on obtient $y\overline{U(X)} = \overline{1}$ et ainsi $y^{-1} = \overline{X^2 - \frac{5}{2}X + 5}$.*

**Exercice 5.14** *Soient $K$ un corps (commutatif) de caractéristique différente de deux et $P(X, Y, Z)$ un polyôme élément de $K[X, Y, Z]$ vérifiant $P(X, Y, Z) = -P(-X, Y, Z)$.*

*Montrer qu'il existe un polynôme $Q(X, Y, Z)$ élément de $K[X, Y, Z]$ tel que $P(X, Y, Z) = XQ(X^2, Y, Z)$ (Ind : considérer $P(X, Y, Z)$ comme un polynôme en $X$ à coefficients dans l'anneau $K[Y, Z]$).*

**Solution**

*On considère $P(X, Y, Z) = S(X) = \sum_{k=0}^{n} a_k(Y, Z)X^k$, avec $a_k(Y, Z) \in K[Y, Z]$, comme un polynôme à une indéterminée $X$ et à coefficients dans $A = K[Y, Z]$. Alors $S(-X) = \sum_{k=0}^{n}(-1)^k a_k(Y, Z)X^k = -\sum_{k=0}^{n} a_k(Y, Z)X^k$, ainsi pour les monômes de degré un entier pair $k$, on obtient $a_k(Y, Z) = -a_k(Y, Z)$ et donc $a_k(Y, Z) = 0$ car $car(K) \neq 2$ d'où $S(X) = a_1(Y, Z)X + a_3(Y, Z)X^3 + ... + a_{2m+1}(Y, Z)X^{2m+1}$ ($2m+1 = n$ si $n$ est impair et $2m+1 = n-1$ si $n$ est pair). Alors, $P(X, Y, Z) = S(X) = X(a_1(Y, Z) + a_3(Y, Z)X^2 + ... + a_{2m+1}(Y, Z)(X^2)^m) = XQ(X^2, Y, Z)$, avec $Q(X, Y, Z) = a_1(Y, Z) + a_3(Y, Z)X + ... + a_{2m+1}(Y, Z)X^m$.*

**Exercice 5.15** *Soit $P = X^2Y + X^2Z + Y^2X + Y^2Z + Z^2X + Z^2Y \in \mathbb{C}[X, Y, Z]$.*

*1) Vérifier que $P$ est un polynôme symétrique.*

*2) Exprimer $P(X, Y, Z)$ sous la forme $Q(\sigma_1, \sigma_2, \sigma_3)$, où $Q(X, Y, Z) \in \mathbb{C}[X, Y, Z]$ et $\sigma_1, \sigma_2, \sigma_3$ les polynômes symétriques élémentaires.*

*Application : Soient $\alpha, \beta$ et $\gamma$ les racines dans $\mathbb{C}$ de l'équation $x^3 + x - 2 = 0$. Calculer $P(\alpha, \beta, \gamma)$.*

**Solution**

*1) On a $P(Y, X, Z) = P(Z, Y, X) = P(X, Y, Z)$ et alors $P$ est symétrique.*

*2) On a $P(X, Y, Z) = XY(X + Y + Z) + XZ(X + Y + Z) + YZ(X + Y + Z) - 3XYZ = (XY + XZ + YZ)(X + Y + Z) - 3XYZ = \sigma_1.\sigma_2 - 3\sigma_3 = Q(\sigma_1, \sigma_2, \sigma_3)$, où $Q(X, Y, Z) = XY - 3Z$.*

*Application : on a $X^3 + X - 2 = (X - \alpha)(X - \beta)(X - \gamma) = X^3 - \sigma_1(\alpha, \beta, \gamma)X^2 + \sigma_2(\alpha, \beta, \gamma)X - \sigma_3(\alpha, \beta, \gamma)$. Alors, $\sigma_1(\alpha, \beta, \gamma) = 0$, $\sigma_2(\alpha, \beta, \gamma) = 1$ et $\sigma_3(\alpha, \beta, \gamma) = 2$. D'autre part, on a $P(\alpha, \beta, \gamma) = \sigma_1(\alpha, \beta, \gamma).\sigma_2(\alpha, \beta, \gamma) - 3\sigma_3(\alpha, \beta, \gamma)$ d'où $P(\alpha, \beta, \gamma) = 0.1 - 3.2 = -6$.*

# Chapitre 6

# Sujets d'examens

## 6.1 Côntrole final (2006-2007)

**Exercice 6.1** *Un groupe $G$ est dit <u>métacyclique</u> s'il existe un sous groupe $H$ de $G$ cyclique, distingué dans $G$ et tel que $G/H$ est un groupe cyclique.*

*1) Soient $G = < a >$ un groupe cyclique d'ordre $n$ et $H$ un sous-groupe de $G$.*

*a) Dire pourquoi $H$ est distingué dans $G$.*

*b) Montrer que $H$ est cyclique.*

*c) Montrer que $G/H$ est cyclique.*

*d) Conclure.*

*2) Montrer que $S_3$ est un groupe métacyclique mais que $S_3$ n'est pas cyclique. (Ind. pour montrer que $S_3$ est métacyclique, on prend $H =< c >$, où $c$ est un 3-cycle de $S_3$).*

*3) Soit $G$ un groupe métacyclique. i.e., il existe un sous groupe $H$ de $G$ cyclique, distingué dans $G$ et tel que $G/H$ est un groupe cyclique. Soit $K$ un sous-groupe de $G$.*

*a) Montrer que $H \cap K$ est un sous-groupe cyclique et distingué de $K$.*

*b) Montrer que $K/H \cap K$ est cyclique. (Ind. utiliser le deuxième théorème d'isomorphisme et la question 1) b)).*

*c) Conclure.*

**Exercice 6.2** *On désigne par $A$ l'anneau $A = \mathbb{Z}[i\sqrt{7}] = \{a + ib\sqrt{7}/a, b \in \mathbb{Z}\}$.*

*1) Déterminer $\mathcal{U}(A)$ et $Fr(A)$.*

*2) Montrer que les éléments 2, $1 + i\sqrt{7}$ et $1 - i\sqrt{7}$ sont irréductibles dans $A$.*

*3) En considérant $2^3$ et $(1 + i\sqrt{7})(1 - i\sqrt{7})$, montrer que $A$ n'est pas principal.*

**Exercice 6.3**

***I**) Soient $A$ et $B$ deux anneaux commutatifs unitaires, $f : A \longrightarrow B$ un homomorphisme d'anneaux <u>surjectif</u>. On se propose de montrer que si $\mathfrak{m}$ est un idéal maximal de $B$ alors $f^{-1}(\mathfrak{m})$ est un idéal maximal de $A$.*

*1) Soit $I$ un idéal de $A$.*

*a) Montrer que $f(I)$ est un idéal de $B$.*

*b) Soit $\bar{f} : A/I \longrightarrow B/f(I)$, $\bar{a} = a + I \longmapsto \overline{f(a)} = f(a) + f(I)$.*

*i) Montrer que $\bar{f}$ est une application bien définie et que $\bar{f}$ est un homomorphisme d'anneaux surjectif.*

*ii) Montrer que si $\ker f \subset I$, alors $\bar{f}$ est un isomorphisme.*

*2) Soit $\mathfrak{m}$ un idéal maximal de $B$ et $J = f^{-1}(\mathfrak{m})$.*

*a) Dire pourquoi* $J$ *est un idéal de* $A$.

*b) Montrer que* $\ker f \subset J$ *et que* $f(J) = \mathfrak{m}$.

*c) Montrer que* $J = f^{-1}(\mathfrak{m})$ *est un idéal maximal de* $A$. *(Ind. Utiliser 1) b) ii)).*

***II****) On considère l'anneau* $\mathbb{Z}[X]$ *de polynômes à une indéterminée à coefficients dans* $\mathbb{Z}$.

*1)*

*a) Déterminer* $\mathcal{U}(\mathbb{Z}[X])$ *et* $\mathcal{U}((\mathbb{Z}/2\mathbb{Z})[X])$.

*b) Montrer que* $Q(X) = X^3 + X + \overline{1} \in (\mathbb{Z}/2\mathbb{Z})[X]$ *est un polynôme irréductible dans* $(\mathbb{Z}/2\mathbb{Z})[X]$.

*c) Montrer que le polynôme* $P(X) = 15X^3 + 12X^2 + 9X + 27$ *est irréductible dans* $\mathbb{Q}[X]$.

*d) Le polynôme* $P(X)$ *est-il irréductible dans* $\mathbb{Z}[X]$ *?*

*2) On considère l'homomorphisme d'anneaux surjectif* $\varphi : \mathbb{Z}[X] \longrightarrow (\mathbb{Z}/2\mathbb{Z})[X]$, $\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} \overline{a_i} X^i$, *où* $\overline{a_i}$ *désigne la classe de* $a_i$ *modulo* 2.

*a) Montrer que* $\ker \varphi = (2) = 2.\mathbb{Z}[X]$.

*b) Dire pourquoi l'idéal* $\mathfrak{m} = (Q) = Q.(\mathbb{Z}/2\mathbb{Z})[X]$ *de* $(\mathbb{Z}/2\mathbb{Z})[X]$ *est un idéal maximal.*

*c) Montrer que* $\varphi^{-1}(\mathfrak{m}) = 2.\mathbb{Z}[X] + P.\mathbb{Z}[X]$. *(ind. pour* $\varphi^{-1}(\mathfrak{m}) \subset 2.\mathbb{Z}[X] + P.\mathbb{Z}[X]$, *remarquer que* $Q = \varphi(P)$ *et que* $\varphi$ *est surjectif).*

*d) En déduire que* $2.\mathbb{Z}[X] + P.\mathbb{Z}[X]$ *est un idéal maximal de* $\mathbb{Z}[X]$. *(Ind. Utiliser I). 2)).*

**Solution**

***Exercice 6.1 :***

*1)*

*a) Puisque* $G$ *est cyclique,* $G$ *est abélien et ainsi* $H \lhd G$.

*b) Si* $H = \{e\}$, *alors* $H =< e >$ *est cyclique. On suppose alors que* $H$ *est un sous-groupe de* $G$ *différent de* $\{e\}$. *D'où il existe un plus petit entier* $m$ *strictement positif tel que* $a^m \in H$ *et alors* $< a^m > \subset H$. *D'autre part, si* $x \in H$, *alors* $\exists s \in \mathbb{Z} : x = a^s$ *car* $H \subset G =< a >$. *En effectuant la division euclidienne de* $s$ *par* $m$, $\exists!(q, r) \in \mathbb{Z}^2 : s = qm + r$ *avec* $0 \leq r < m$ *ainsi* $a^r = a^{s-qm} = a^s(a^m)^{-q} \in H$ *et alors* $r = 0$ *car* $m$ *est le plus petit entier strictement positif tel que* $a^m \in H$ *et ceci prouve que* $x = a^s = (a^m)^q \in < a^m >$. *Ainsi, puisque* $H$ *est monogène et fini, alors* $H$ *est cyclique.*

*c) On a* $G/H =< \overline{a} >$. *En effet, puisque* $< \overline{a} > \subset G/H$, *il suffit de vérifier que* $G/H \subset < \overline{a} >$. *Soit* $\bar{x} \in G/H$, *comme* $x \in G$ *et* $G = < a >$, *alors* $\exists m \in \mathbb{Z} : x = a^m$ *d'où* $\bar{x} = \overline{a^m} = \overline{a}^m \in < \overline{a} >$. *Comme* $G$ *est fini,* $H$ *est fini et alors* $|G/H| = \frac{|G|}{|H|}$ *est fini.*

*d) Tout groupe cyclique est métacyclique.*

*2) Soient* $c$ *un 3-cycle de* $S_3$ *et* $H =< c >$ *le sous-groupe cyclique de* $S_3$ *engendré par* $c$. *On a* $H \lhd S_3$ *car* $[S_3 : H] = \frac{6}{3} = 2$. *Comme le groupe quotient* $S_3/H$ *est d'ordre* 2, $S_3/H$ *est cyclique. Ainsi,* $S_3$ *est un groupe métacyclique. Cependant, puisque* $S_3$ *n'est pas abélien,* $S_3$ *n'est pas cyclique.*

*3)*

*a) On a* $H \cap K$ *est un sous-groupe de* $G$ *et* $H \cap K \subset K$ *d'où* $H \cap K$ *est un sous-groupe de* $K$.

*Vérifions que* $H \cap K \lhd K$ *:* $\forall k \in K, \forall x \in H \cap K$, *on a* $kxk^{-1} \in H$ *car* $x \in H$, $k \in K \subset G$ *et* $H \lhd G$ *et on a aussi* $kxk^{-1}$ *car* $x \in K$, $k \in K$ *et* $K$ *est un sous-groupe de* $G$. *D'où* $kxk^{-1} \in H \cap K$.

*Remarque : On peut remarquer aussi que puisque $H \lhd G$ et $K$ est un sous-groupe de $G$, alors, d'après le $2^{\text{ème}}$ théorème d'isomorphisme, $H \cap K \lhd K$.*

*D'autre part, $H \cap K$ est un sous-groupe de $H$ et puisque $H$ est cyclique, on a, d'après la question 1)b), $H \cap K$ est cyclique.*

*b) On a, d'après le le $2^{\text{ème}}$ théorème d'isomorphisme, $K/H \cap K \simeq HK/H$. Comme $HK/H$ est un sous-groupe de $G/H$ et $G/H$ est cyclique, on a, d'après 1)b), $HK/H$ est cyclique et par suite $K/H \cap K$ est cyclique.*

*c) $K$ est métacyclique et ainsi tout sous-groupe d'un groupe métacyclique est métacyclique.*

***Exercice 6.2 :***

*1) $\mathcal{U}(A) = \{-1, 1\}$ et $Fr(A) = \{\alpha + i\beta\sqrt{7}/\alpha, \beta \in \mathbb{Q}\} = \mathbb{Q}[i\sqrt{7}]$ $(= \mathbb{Q}(i\sqrt{7}))$.*

*2) * 2 est non nul et non inversible. Soit $x = a + ib\sqrt{7} \in A : x/2$ d'où $\exists y = c + id\sqrt{7} \in A : 2 = xy$ alors $4 = |xy|^2 = |x|^2|y|^2 = (a^2 + 7b^2)(c^2 + 7d^2)$. Puisque $a^2 + 7b^2$ et $c^2 + 7d^2 \in \mathbb{N}$, $a^2 + 7b^2 \in \{1, 2, 4\}$. Or, $\forall a, b \in \mathbb{Z}$, $a^2 + 7b^2 \neq 2$ d'où $a^2 + 7b^2 \in \{1, 4\}$.*

*Si $a^2 + 7b^2 = 1$, alors $x = a + ib\sqrt{7} = \pm 1 \in \mathcal{U}(A)$ et si $a^2 + 7b^2 = 4$, alors $c^2 + 7d^2 = 1$ d'où $y = c + id\sqrt{7} = \pm 1 \in \mathcal{U}(A)$. Ainsi 2 est irréductible dans $A$.*

** $1 \pm i\sqrt{7}$ est non nul et non inversible. Soit $x = a + ib\sqrt{7} \in A : x/1 \pm i\sqrt{7}$ d'où $\exists y = c + id\sqrt{7} \in A : 1 \pm i\sqrt{7} = xy$ alors $8 = |xy|^2 = |x|^2|y|^2 = (a^2 + 7b^2)(c^2 + 7d^2)$. Puisque $a^2 + 7b^2$ et $c^2 + 7d^2 \in \mathbb{N}$, $a^2 + 7b^2 \in \{1, 2, 4, 8\}$. Or, $\forall a, b \in \mathbb{Z}$, $a^2 + 7b^2 \neq 2$ et on a aussi $a^2 + 7b^2 \neq 4$, sinon $c^2 + 7d^2 = 2$, ce qui est impossible car $c, d \in \mathbb{Z}$. D'où $a^2 + 7b^2 \in \{1, 8\}$.*

*Si $a^2 + 7b^2 = 1$, alors $x = a + ib\sqrt{7} = \pm 1 \in \mathcal{U}(A)$ et aussi si $a^2 + 7b^2 = 4$, alors $c^2 + 7d^2 = 1$ d'où $y = c + id\sqrt{7} = \pm 1 \in \mathcal{U}(A)$. Ainsi $1 \pm i\sqrt{7}$ est irréductible dans $A$.*

*3) On a $8 = 2^3 = (1 + i\sqrt{7})(1 - i\sqrt{7})$ et on remarque que dans la première décomposition de 8 en facteurs irréductibles $8 = 2^3$, on 3 facteurs irréductibles. Cependant, dans la deuxième décomposition $8 = (1 + i\sqrt{7})(1 - i\sqrt{7})$, on n'a que 2 facteurs irréductibles. Alors, $A$ n'est pas principal.*

*Remarque : * On peut aussi vérifier que 2 n'est pas associé ni à $1 + i\sqrt{7}$ ni à $1 - i\sqrt{7}$.*

** Aussi, on peut remarquer que 2 est irréductible mais 2 n'est pas premier : il suffit de vérifier que $2/8 = (1 + i\sqrt{7})(1 - i\sqrt{7})$ mais $2 \nmid 1 + i\sqrt{7}$ et $2 \nmid 1 - i\sqrt{7}$ car si $2/1 + i\sqrt{7}$ (ou $2/1 - i\sqrt{7}$), $2 \in \mathcal{U}(A)$, ce qui est faux.*

***Exercice 6.3 :***

***I)**1)*

*a) cf. exercice 3.4)1)b).*

*b)*

*i) On a $\forall \bar{a} = a + I \in A/I, f(a) \in B$ et donc $\overline{f(a)} = f(a) + f(I) \in B/f(I)$. Supposons que $\bar{a} = \bar{b}$, alors $a - b \in I$ d'où $f(a - b) = f(a) - f(b) \in f(I)$, i.e., $\overline{f(a)} = \overline{f(b)}$ dans $B/f(I)$ et ainsi $\bar{f}(\bar{a}) = \bar{f}(\bar{b})$.*

*Montrons que $\bar{f}$ est un homomorphisme d'anneaux : on a $\forall \bar{a}, \bar{b} \in A/I$, $\bar{f}(\bar{a} + \bar{b}) = \bar{f}(\overline{a + b}) = \overline{f(a + b)} = \overline{f(a) + f(b)} = \overline{f(a)} + \overline{f(b)} = \bar{f}(\bar{a}) + \bar{f}(\bar{b})$. De même, $\bar{f}(\bar{a}.\bar{b}) = \bar{f}(\bar{a}).\bar{f}(\bar{b})$ et on a aussi $\bar{f}(\overline{1_A}) = \overline{f(1_A)} = \overline{1_B}$.*

*$\bar{f}$ est surjectif. En effet, $\forall \bar{d} \in B/f(I)$, $d \in B$ d'où $\exists c \in A : f(c) = d$ car $f$ est surjectif. Ainsi, $\bar{d} = \overline{f(c)} = \bar{f}(\bar{c})$ avec $\bar{c} \in A/I$.*

*ii) Soit $\bar{a} \in \ker \bar{f}$ d'où $\bar{f}(\bar{a}) = \overline{f(a)} = \bar{0} = 0 + f(I)$ alors $f(a) \in f(I)$, i.e., $\exists x \in I : f(a) = f(x)$ d'où $f(a - x) = f(a) - f(x) = 0$ ainsi $a - x \in \ker f \subset I$ et par suite $a \in I$ car $a - x \in I$, $x \in I$ et $I$ est un idéal de $A$. Alors, $\bar{a} = \bar{0}$ dans $A/I$ et donc $\ker \bar{f} \subset \{\bar{0}\}$. Comme $\{\bar{0}\} \subset \ker \bar{f}$, $\ker \bar{f} = \{\bar{0}\}$ et ainsi $\bar{f}$ est injectif.*

*2)*

*a) Puisque $f$ est un homomorphisme d'anneaux et $\mathfrak{m}$ est un idéal de $B$, $f^{-1}(\mathfrak{m})$ est un idéal de $A$.*

*b) Soit $x \in \ker f$ alors $f(x) = 0 \in \mathfrak{m}$ et ainsi $x \in f^{-1}(\mathfrak{m}) = J$. D'où $\ker f \subset J$. On a aussi $f(J) = \mathfrak{m}$ car $f$ est une application surjective.*

*c) D'après la question 1)b)ii), on a $A/J \simeq B/f(J)$, i.e. $A/f^{-1}(\mathfrak{m}) \simeq B/\mathfrak{m}$ et comme $B/\mathfrak{m}$ est un corps, $A/f^{-1}(\mathfrak{m})$ est un corps et par suite $f^{-1}(\mathfrak{m})$ est un idéal maximal de $A$.*

***II)** 1)*

*a) Puisque $\mathbb{Z}$ est intègre, $\mathcal{U}(\mathbb{Z}[X]) = \mathcal{U}(\mathbb{Z})$ et donc $\mathcal{U}(\mathbb{Z}[X]) = \{-1, 1\}$.*

*Aussi, puisque $\mathbb{Z}/2\mathbb{Z}$ est un corps, $\mathcal{U}((\mathbb{Z}/2\mathbb{Z})[X]) = (\mathbb{Z}/2\mathbb{Z})^* = \{\overline{1}\}$.*

*b) Puisque $Q(X) = X^3 + X + \overline{1} \in (\mathbb{Z}/2\mathbb{Z})[X]$ est de degré 3 et $(\mathbb{Z}/2\mathbb{Z})$ est un corps, il suffit de vérifier que $Q(X)$ n'a pas de racines dans $(\mathbb{Z}/2\mathbb{Z})$. on a $\tilde{Q}(\overline{0}) = \overline{1}$, $\tilde{Q}(\overline{1}) = \overline{1}$ et ainsi $Q(X)$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$.*

*c) On a $P(X) = 15X^3+12X^2+9X+27 = 3S(X)$ avec $S(X) = 5X^3+4X^2+3X+9 \in \mathbb{Q}[X]$. Comme $P$ et $S$ sont associés dans $\mathbb{Q}[X]$, il suffit de vérifier que $S(X)$ est irréductible dans $\mathbb{Q}[X]$. En effet, $S(X) \in \mathbb{Z}[X]$ est primitif et non constant et $\mathbb{Z}$ est principal. En prenant $p = 2$, on a $p$ est premier dans $\mathbb{Z}$, $p \nmid 5$ et la réduction modulo $p = 2$ de $S(X)$ est $X^3 + X + \overline{1} = Q(X) \in (\mathbb{Z}/2\mathbb{Z})[X]$. Alors, puisque $Q(X)$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$, on a $S(X)$ est irréductible dans $\mathbb{Z}[X]$.*

*En remarquant que $\mathbb{Z}$ est principal, $\mathbb{Q} = Fr(\mathbb{Z})$ et $S(X)$ est non constant et irréductible dans $\mathbb{Z}[X]$, on a $S(X)$ est irréductible dans $\mathbb{Q}[X]$.*

*d) Puisque $P(X)$ n'est pas primitif, $P(X)$ n'est pas irréductible dans $\mathbb{Z}[X]$.*

*2)*

*a) On a $2.\mathbb{Z}[X] \subset \ker\varphi$, alors il suffit de vérifier que $\ker\varphi \subset 2.\mathbb{Z}[X]$. Soit $U(X) = \sum_{i=0}^{n} a_i X^i \in \ker\varphi$, d'où $\varphi(U(X)) = \sum_{i=0}^{n} \overline{a_i} X^i = \overline{0}$ i.e., $\overline{a_i} = \overline{0}$ $\forall i$, d'où $a_i = 2b_i$, avec $b_i \in \mathbb{Z}$. Alors $U(X) = \sum_{i=0}^{n} a_i X^i = 2.\sum_{i=0}^{n} b_i X^i \in 2.\mathbb{Z}[X]$.*

*b) L'anneau $(\mathbb{Z}/2\mathbb{Z})[X]$ est principal car $(\mathbb{Z}/2\mathbb{Z})$ est un corps et $Q$ est irréductible dans $(\mathbb{Z}/2\mathbb{Z})[X]$, alors l'idéal $(Q(X))$ est maximal.*

*c) Montrons que $2.\mathbb{Z}[X] + P.\mathbb{Z}[X] \subset \varphi^{-1}(\mathfrak{m})$ : soient $U(X), V(X) \in \mathbb{Z}[X]$. Alors, on a $\varphi(2.U(X) + P.V(X)) = Q(X).\varphi(V(X)) \in (Q(X)) = \mathfrak{m}$ et donc $2.U(X) + P.V(X) \in \varphi^{-1}(\mathfrak{m})$. Pour l'autre inclusion, soit $U(X) \in \varphi^{-1}(\mathfrak{m})$, d'où $\varphi(U(X)) \in \mathfrak{m} = (Q(X))$, i.e., $\varphi(U(X)) = Q(X).V(X)$, où $V(X) \in (\mathbb{Z}/2\mathbb{Z})[X]$. Comme $V(X) = \varphi(V'(X))$, où $V'(X) \in \mathbb{Z}[X]$, car $\varphi$ est surjectif et puisque $\varphi(P(X)) = Q(X)$, alors $\varphi(U(X)) = \varphi(P(X)).\varphi(V'(X)) = \varphi(P(X).V'(X))$ d'où $\varphi(U(X) - P(X).V(X)) = 0$, i.e., $U(X) - P(X).V(X) \in \ker\varphi = 2.\mathbb{Z}[X]$. Ainsi $U(X) = 2.\mathbb{Z}[X] + P.\mathbb{Z}[X]$.*

*d) Puisque $\varphi$ est un homomorphisme d'anneaux surjectif et $\mathfrak{m}$ est un idéal maximal de $(\mathbb{Z}/2\mathbb{Z})[X]$, alors, d'après la question I)2), $2.\mathbb{Z}[X] + P.\mathbb{Z}[X] = \varphi^{-1}(\mathfrak{m})$ est un idéal maximal de $\mathbb{Z}[X]$.*

## 6.2 Rattrapage (2006-2007)

**Exercice 6.4** *Soient $p \in \mathbb{N}$ un nombre premier et $a \in \mathbb{Z}$ tels que $p$ ne divise pas $a$.*

*1) Montrer que $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{a}, \overline{2a} ..., \overline{(p-1)a}\}$. (Ind. on vérifiera que si $i, j \in \{0, 1, ..., p-1\}$ tels que $i \neq j$, alors $\overline{ia} \neq \overline{ja}$).*

*2) En déduire* $(p-1)!a^{p-1} \equiv (p-1)! \pmod p$.

*3) Montrer que* $a^{p-1} \equiv 1 \pmod p$.

*4) Application : Montrer que pour tout entier* $a \geq 2$, $a^7 - a$ *est divisible par* $42 = 2.3.7$. *(Ind. utiliser 3) et* $a^7 - a = a(a^6 - 1) = \ldots$*).*

**Exercice 6.5** *Soit* $G$ *un groupe fini d'ordre* $n > 1$ *d'élément neutre* $e$. *On désigne par* $N = \{t \in \mathbb{N}^* : \forall x \in G, x^t = e\}$.

*1) Montrer que* $N$ *n'est pas vide.*

*On pose* $m = \inf N$.

*2) Montrer que pour* $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *on a :* $m < n$ *et déterminer* $m$ *pour* $S_3$.

*3) Montrer que si* $t \in N$, *alors* $m$ *divise* $t$ *et qu'ainsi* $m$ *divise* $n$.

*4) Montrer que* $m = ppcm(o(x)/x \in G)$.

*5) On suppose que* $G$ *est commutatif, que* $m = rs$ *avec* $r > 1$, $s > 1$ *et que* $r \wedge s = 1$. *On pose* $H = \{x \in G : x^r = e\}$, $K = \{x \in G : x^s = e\}$.

*a) Montrer que* $H$ *et* $K$ *sont des sous-groupes de* $G$.

*b) Montrer que* $H \cap K = \{e\}$, $HK = G$ *et qu'ainsi* $G$ *est isomorphe à* $H \times K$.

*c) Montrer que* $H \neq \{e\}$, $K \neq \{e\}$.

**Exercice 6.6** *On considère l'anneau* $A = \mathbb{Z}[i\sqrt{p}] = \{a + ib\sqrt{p}/a, b \in \mathbb{Z}\}$, *où* $p \in \mathbb{N}$ *est un nombre premier, et l'application* $f : A = \mathbb{Z}[i\sqrt{p}] \to \mathbb{Z}/(p+1)\mathbb{Z}$, $a + ib\sqrt{p} \longmapsto \overline{a + pb}$.

*1) Montrer que* $f$ *est un homomorphisme d'anneaux surjectif.*

*2)*

*a) Montrer que* $p+1 \in (1+i\sqrt{p})$, *où* $(1+i\sqrt{p})$ *est l'idéal de* $A$ *engendré par* $1+i\sqrt{p}$.

*b) En déduire que* $\ker f = (1+i\sqrt{p})$.

*3)*

*a) On suppose que* $p = 2$. *L'idéal* $(1+i\sqrt{2})$ *de* $A$ *est-il maximal ?* $1+i\sqrt{2}$ *est-il premier ?*

*b) On suppose que* $p \neq 2$. *L'idéal* $(1+i\sqrt{p})$ *de* $A$ *est-il premier ?* $1+i\sqrt{p}$ *est-il premier ?*

**Exercice 6.7**

*1) Soient* $A$ *un anneau commutatif unitaire et* $B$ *un sous-anneau de* $A$. *Montrer que si* $I$ *est un idéal premier de* $A$ *et* $I \cap B \neq B$ *alors* $I \cap B$ *est un idéal premier de* $B$.

*On considère l'anneau* $\mathbb{Z}[X]$ *des polynômes à une indéterminée à coefficients dans* $\mathbb{Z}$ *et l'anneau* $\mathbb{Q}[X]$ *des polynômes à une indéterminée à coefficients dans* $\mathbb{Q}$.

*2)*

*a) Montrer que le polynôme* $P(X) = X^4 + 15X^3 + 9X + 3 \in \mathbb{Z}[X]$ *est irréductible dans* $\mathbb{Z}[X]$.

*b) En déduire que le polynôme* $Q(X) = \frac{2}{5}X^4 + 6X^3 + \frac{18}{5}X + \frac{6}{5} \in \mathbb{Q}[X]$ *est irréductible dans* $\mathbb{Q}[X]$.

*3) Soit* $I = P(X).\mathbb{Q}[X]$ *l'idéal de* $\mathbb{Q}[X]$ *engendré par* $P(X)$. *Dire pourquoi* $I = P(X).\mathbb{Q}[X]$ *est un idéal premier de* $\mathbb{Q}[X]$.

*4) Soit* $J = I \cap \mathbb{Z}[X]$. *Montrer que* $J$ *est un idéal premier de* $\mathbb{Z}[X]$. *(Ind. utiliser 1)).*

**Solution**

***Exercice 6.4 :***

*1) Soient* $i, j \in \{0, 1, ..., p-1\}$ *tels que* $\overline{ia} = \overline{ja}$, *alors* $p/a(i-j)$ *et puisque* $p \wedge a = 1$, *on a* $p/i-j$. *Or* $0 \leq |i-j| \leq p-1$, *donc* $i-j = 0$, *i.e.,* $i = j$. *Ainsi card*$\{\overline{0}, \overline{a}, \overline{2a} ..., \overline{(p-1)a}\} = p$.

*Puisque* $\{\overline{0}, \overline{a}, \overline{2a}..., \overline{(p-1)a}\} \subset \mathbb{Z}/p\mathbb{Z}$ *et* $card(\mathbb{Z}/p\mathbb{Z}) = \{\overline{0}, \overline{a}, \overline{2a}..., \overline{(p-1)a}\} = p$, *on a* $\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{a}, \overline{2a}..., \overline{(p-1)a}\}$.

*2) D'après 1), on a* $(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{1}, ..., \overline{p-1}\} = \{\overline{a}, \overline{2a}..., \overline{(p-1)a}\}$ *d'où* $\overline{1}.....\overline{p-1} = \overline{a}.\overline{2a}...,.\overline{(p-1)a}$, *i.e.,* $(p-1)! \equiv (p-1)!a^{p-1}(\mathrm{mod}\, p)$.

*3) D'après 2),* $p/(p-1)!(a^{p-1}-1)$ *et comme* $p \nmid (p-1)!$, *alors* $p/(a^{p-1}-1)$, *i.e.,* $a^{p-1} \equiv 1$ $(\mathrm{mod}\, p)$.

*4) En posant* $p = 7$, *on a ,d'après 3),* $7/a^6 - 1$ *et par suite* $7/a^7 - a = a(a^6-1)$. *De même,* $3/a^3 - a$ *et comme* $a^3 - a/a^7 - a$ $(a^7 - a = (a^3-a)(a^4+a^2+1))$, *on a* $3/a^7 - a$. *Aussi,* $2/a^2 - a$ *et comme* $a^2 - a/a^7 - a$ $(a^7 - a = (a^2-a)(a^5+a^4+a^3+a^2+a+1))$, *on a* $2/a^7 - a$. *Ainsi* $42 = 2.3.7/a^7 - a$.

***Exercice 6.5 :***

*1)* $N$ *n'est pas vide car* $n \in N$.

*2) On remarque que* $m \leq n$ *car* $n \in N$ *et* $m = \inf N$.

** Pour* $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, *on a* $n = 4$. *D'autre part, puisque* $G \neq \{e\}$ *et* $\forall (\bar{x}, \bar{y}) \in G, 2.(\bar{x}, \bar{y}) = (\bar{0}, \bar{0})$, $m = 2$.

** Pour* $S_3$, *on a* $n = 6$. *D'autre part, si* $\sigma \in S_3$, *on a* $\sigma^m = e$. *Alors, en prenant* $\sigma = \tau$, *où* $\tau$ *est une transposition de* $S_3$, *on obtient* $2/m$ *car* $\circ(\tau) = 2$. *De même, en prenant* $\sigma = c$, *où* $c$ *est un 3-cycle de* $S_3$, *on obtient* $3/m$ *car* $\circ(c) = 3$. *Ainsi,* $6/m$ *et puisque* $m \leq n = 6$, $m = 6$.

*3) En effectuant la division euclidienne de* $t$ *par* $m$, *on obtient* $q, r \in \mathbb{N} : t = mq + r$ *avec* $r < m$. *Alors,* $\forall x \in G, e = x^t = (x^m)^q.x^r$ *et puisque* $x^m = e$, *on a* $x^r = e$ *et ceci* $\forall x \in G$. *Vu que* $m = \inf N$ *et* $r < m$, *on a* $r = 0$. *Par conséquent et comme* $n \in N$, *on a* $m/n$.

*4) Posons* $l = ppcm(o(x)/x \in G)$. *Alors* $\forall x \in G, o(x)/l$ *d'où* $x^l = e$ *ainsi* $l \in N$ *et par suite, d'après 3),* $m/l$. *D'autre part,* $\forall x \in G, x^m = e$ *d'où* $\forall x \in G, o(x)/m$ *et ainsi* $l/m$.

*5)*

*a) Montrons que* $H$ *est un sous-groupe de* $G$ *: on a* $H \subset G$, $H \neq \emptyset$ *car* $e \in H$, *et* $\forall x, y \in H$, *on a* $(xy^{-1})^r = x^r y^{-r}$ *car* $G$ *est abélien et donc* $(xy^{-1})^r = e.e = e$ *d'où* $xy^{-1} \in H$. *De même, on vérifie que* $K$ *est un sous-groupe de* $G$.

*b) Soit* $x \in H \cap K$, *alors* $x^r = e$ *et* $x^s = e$ *d'où* $\circ(x)/r$ *et* $\circ(x)/s$ *et par suite* $\circ(x) = 1$ *car* $r \wedge s = 1$.

*On a aussi* $HK = G$. *En effet, puisque* $HK \subset G$, *il suffit de vérifier que* $G \subset HK$. *Pour ceci, puisque* $r \wedge s = 1$, $\exists u, v \in \mathbb{Z} : ur + vs = 1$. *Ainsi,* $\forall g \in G$, $g = g^{vs+ur} = g^{vs}g^{ur}$. *Or,* $(g^{vs})^r = g^{mv} = e$ *et* $(g^{ur})^s = g^{mu} = e$, *i.e.,* $g^{vs} \in H$ *et* $g^{ur} \in K$.

*Ainsi, en considérant* $f : H \times K \longrightarrow G, (h, k) \longmapsto hk$, *on vérifie facilement que* $f$ *est un isomorphisme de groupes.*

*c) On suppose que* $H = \{e\}$. *Alors* $G = K$ *et par suite* $\forall x \in G, x^s = e$ *d'où* $m/s$ *et puisque* $s/m$, $s = m$, *ce qui est faux car* $r > 1$. *De même, on montre que* $K \neq \{e\}$.

***Exercice 6.6 :***

*1) Soient* $x = a + ib\sqrt{p}, y = c + id\sqrt{p} \in \mathbb{Z}[i\sqrt{p}]$, *on a* $f(x+y) = f((a+c) + i(b+d)\sqrt{p}) = \overline{(a+c) + p(b+d)} = \overline{(a+pb)} + \overline{(c+pd)} = f(x) + f(y)$. *Aussi,* $f(x.y) = f(ac - bdp + i(ad+bc)\sqrt{p}) = \overline{(ac-bdp) + p(ad+bc)} = \overline{(ac+bdp^2) + p(ad+bc)}$ *car* $p^2 \equiv -p(\mathrm{mod}\, p+1)$ *et ainsi* $f(x.y) = \overline{(a+bp)(c+pd)} = f(x).f(y)$. *On remarque aussi que* $f(1) = \overline{1}$ *et que* $f$ *est évidemment surjective.*

*2)*

*a) On a* $p + 1 = (1 + i\sqrt{p})(1 - i\sqrt{p})$ *d'où* $p + 1 \in (1 + i\sqrt{p})$.

*b) Il est évident que* $(1+i\sqrt{p}) \subset \ker f$. *Montrons que* $\ker f \subset (1+i\sqrt{p})$. *Soit* $x = a+ib\sqrt{p} \in$

$\ker f$, *alors* $f(x) = \overline{(a+bp)} = \bar{0}$ *d'où* $a + bp = k(p+1)$, *où* $k \in \mathbb{Z}$. *Donc* $x = a + ib\sqrt{p} = (k(p+1) - bp) - b + b + (ib\sqrt{p}) = k(p+1) - b(p+1) + b(1+i\sqrt{p}) = (k-b)(p+1) + b(1+i\sqrt{p}) \in (1+i\sqrt{p})$ *car* $p + 1 \in (1 + i\sqrt{p})$.

*3)*

*a) En appliquant le 1^er théorème d'isomorphisme et en prenant* $p = 2$, *on obtient* $\mathbb{Z}[i\sqrt{p}]/(1+i\sqrt{2}) \simeq \mathbb{Z}/3\mathbb{Z}$, *d'où* $(1+i\sqrt{2})$ *est un idéal maximal et par suite* $(1+i\sqrt{2})$ *est premier et donc l'élément* $1 + i\sqrt{2}$ *est premier.*

*b) En appliquant le 1^er théorème d'isomorphisme, on obtient* $\mathbb{Z}[i\sqrt{p}]/(1+i\sqrt{p}) \simeq \mathbb{Z}/(p+1)\mathbb{Z}$. *Comme* $p$ *est premier et* $p \neq 2$, $p + 1$ *n'est pas premier car* $p + 1$ *est pair et* $p + 1 \neq 2$. *D'où* $\mathbb{Z}[i\sqrt{p}]/(1 + i\sqrt{p})$ *n'est pas intègre et par suite l'idéal* $(1 + i\sqrt{p})$ *n'est pas premier et par conséquent l'élement* $1 + i\sqrt{p}$ *n'est pas premier.*

***Exercice 6.7 :***

*1) D'après le cours,* $I \cap B$ *est un idéal de* $B$. *Montrons que* $I \cap B$ *est premier. Soient* $a, b \in B : ab \in I \cap B$, *alors* $ab \in I$ *et puisque* $I$ *est premier,* $a \in I$ *ou* $b \in I$ *et ainsi* $a \in I \cap B$ *ou* $b \in I \cap B$. *Comme* $I \cap B \neq B$, *alors* $I \cap B$ *est un idéal premier de* $B$.

*2)*

*a) Il suffit d'appliquer le critère d'Eisenstein en prenant* $p = 3$.

*b) Puisque* $P(X)$ *est irréductible dans* $\mathbb{Z}[X]$, $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$ *et par suite* $Q(X) = \frac{2}{5}X^4 + 6X^3 + \frac{18}{5}X + \frac{6}{5} = \frac{2}{5}.P(X)$ *est irréductible dans* $\mathbb{Q}[X]$ *car* $Q \sim P$ *sont associés dans* $\mathbb{Q}[X]$.

*3) Puisque* $P(X)$ *est irréductible dans* $\mathbb{Z}[X]$, $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$*et omme* $\mathbb{Q}[X]$ *est un anneau principal, l'idéal* $I = (P(X)) = P(X).\mathbb{Q}[X]$ *est maximal dans* $\mathbb{Q}[X]$ *et par suite* $I$ *est premier.*

*4) On a* $B = \mathbb{Z}[X]$ *est un sous-anneau de l'anneau* $A = \mathbb{Q}[X]$. *vu que* $I$ *est un idéal premier de* $A = \mathbb{Q}[X]$ *(question 3)), on a, d'après 1),* $I \cap B = J = I \cap \mathbb{Z}[X]$ *est un idéal premier de* $B = \mathbb{Z}[X]$.

## 6.3 Côntrole final (2007-2008)

**Exercice 6.8**

*1) Soient* $A$ *un anneau intègre,* $a, b \in A - \{0\}$ *ayant un ppcm noté* $m$. *Montrer que* $(m) = (a) \cap (b)$.

*2) On pose* $A = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5}/\ a, b \in \mathbb{Z}\}$.

*a) Montrer que* 1 *est un pgcd de* 3 *et* $2 + i\sqrt{5}$ *dans* $A$.

*b) Montrer que* $A \neq (3) + (2 + i\sqrt{5})$.

*c) A est-il principal ?*

**Exercice 6.9** *On considère l'anneau* <u>*principal*</u> $A = \mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2}/\ a, b \in \mathbb{Z}\}$.

*1) Vérifier que* $Fr(A) = \mathbb{Q}[i\sqrt{2}] = \{a + ib\sqrt{2}/\ a, b \in \mathbb{Q}\}$.

*2) Soit* $x = a + ib\sqrt{2} \in A$. *On pose* $N(x) = a^2 + 2b^2$.

*a) Déterminer* $\mathfrak{U}(A)$.

*b) Montrer que si* $N(x)$ *est premier dans* $\mathbb{Z}$, *alors* $x$ *est irréductible dans* $A$.

*c) En déduire que* $1 + i\sqrt{2}$ *est premier dans* $A$.

*3) Soit* $P(X) = X^4 + 9X + 3 \in A[X]$.

*a) Montrer que* $P(X)$ *est irréductible dans* $A[X]$.

*b) En déduire que* $P(X)$ *est irréductible dans* $(\mathbb{Q}[i\sqrt{2}])[X]$.

**Exercice 6.10**

***I)*** *Soient* $n \geq 2, m_1, ..., m_n \in \mathbb{N}^*$, $m = ppcm(m_1, ..., m_n)$ *et*

$$m = p_1^{\alpha_1}...p_r^{\alpha_r},\ \alpha_1 \geq 1, ..., \alpha_r \geq 1 \ \textbf{(*)},$$

*la décomposition de* $m$ *en produit de nombres premiers distincts. Montrer que pour tout* $i$*, il existe* $m_j$ *tel que* $p_i^{\alpha_i}/m_j$ *(en remarquant que* $ppcm(m_1, ..., m_n) = ppcm(ppcm(m_1, , ..., m_{n-1}), m_n)$*, raisonner par récurrence sur* $n$*).*

***II)*** *Soit* $G$ *un groupe abélien fini d'ordre* $n \geq 2$ *et d'élément neutre* $e$*.*

*1)*

*a) Soit* $a \in G$ *d'ordre* $m$*. Montrer que si* $d/m$*, alors* $\circ(a^{\frac{m}{d}}) = d$*.*

*b) Soient* $a, b \in G$ *d'ordres respectivement* $m_1$ *et* $m_2$*. Montrer que si* $m_1 \wedge m_2 = 1$*, alors* $< a > \cap < b >= \{e\}$ *et qu'ainsi* $\circ(ab) = m_1 m_2$*.*

*2) On pose* $m = ppcm(\circ(x), x \in G)$ *et on considère* $m = p_1^{\alpha_1}...p_r^{\alpha_l}$, $\alpha_1 \geq 1, ..., \alpha_r \geq 1$*, la décomposition* ***(*)*** *de* $m$*.*

*a) Montrer que pour tout* $i \in \{1, ..., r\}$*, il existe* $a_i \in G$ *tel que* $p_i^{\alpha_i}/\circ(a_i)$ *(ind : utiliser I)).*

*b) En déduire pour tout* $i \in \{1, ..., r\}$*, il existe* $b_i \in G$ *tel que* $\circ(b_i) = p_i^{\alpha_i}$*. (utiliser II)1)a)).*

*c) On pose* $b = b_1 \dots b_r$*. Montrer que* $\circ(b) = p_1^{\alpha_1}...p_r^{\alpha_l} = m$ *(raisonner par récurrence sur* $r$ *et utiliser II)1)b)) et qu'ainsi* $m/n$*.*

*3) Application : Soit* $K$ *un corps (commutatif) fini ayant* $q$ *éléments, avec* $q \geq 3$*. On note* $b$ *un élément du groupe multiplicatif* $K^*$ *tel que* $\circ(b) = m = ppcm(\circ(x)/x \in K^*)$*.*

*a) Dire pourquoi* $m \leq q - 1$*.*

*b) Montrer pour tout* $a \in K^*$*,* $a$ *est racine du polynôme* $X^m - 1 \in K[X]$*.*

*c) En déduire que* $m = q - 1$ *et que* $K^*$ *est cyclique.*

**Solution**

***Exercice 6.8***

*1) On a* $a/m$ *et* $b/m$*, alors* $m \in (a) \cap (b)$ *et ainsi* $(m) \subset (a) \cap (b)$*. D'autre part, si* $x \in (a) \cap (b)$*, alors* $a/x$ *et* $b/x$*, d'où* $m/x$ *et ainsi* $x \in (m)$*.*

*2)*

*a) On a* $1/3$ *et* $1/2 + i\sqrt{5}$*. D'autre part, soit* $x = a + ib\sqrt{5}$ *:* $x/3$ *et* $x/2 + i\sqrt{5}$*, d'où* $\exists y = c + id\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ *tel que* $3 = xy$*, alors* $9 = (a^2+5b^2)(c^2+5d^2)$ *et ainsi* $a^2+5b^2 \in \{1, 3, 9\}$*. Or* $a^2 + 5b^2 \neq 3, \forall a, b \in \mathbb{Z}$*. Aussi,* $a^2 + 5b^2 \neq 9$*, sinon* $c^2 + 5d^2 = 1$*, i.e.,* $y = \pm 1$ *et donc* $x = \pm 3$ *; cependant,* $\pm 3 \nmid 2 + i\sqrt{5}$*. Alors,* $a^2 + 5b^2 = 1$*, i.e.,* $x = \pm 1$*.*

*b) Supposons que* $A = (3) + (2 + i\sqrt{5})$*, i.e.,* $1 \in (3) + (2 + i\sqrt{5})$*, d'où* $1 = 3(a + ib\sqrt{5}) + (2 + i\sqrt{5})(c + id\sqrt{5})$*, alors* $\begin{cases} 1 = & 3a + 2c - 5d \\ 0 = & 3b + 2d + c \end{cases}$ *et ainsi* $1 = 3(a + b + c - d)$*, ce qui est impossible car* $a, b, c, d \in \mathbb{Z}$*.*

*c) Puisque 1 est un pgcd de 3 et* $2 + i\sqrt{5}$ *dans* $A$ *et* $A = (1) \neq (3) + (2 + i\sqrt{5})$*, alors* $A$ *n'est pas principal.*

***Exercice 6.9***

*1) Soit* $x \in Fr(A)$*, alors* $x = \frac{a+ib\sqrt{2}}{c+id\sqrt{2}}$*, avec* $a, b, c, d \in \mathbb{Z}$ *et* $c + id\sqrt{2} \neq 0$ *(i.e.,* $(c, d) \neq (0, 0)$*). Alors* $c - id\sqrt{2} \neq 0$ *et* $x = \frac{(a+ib\sqrt{2})(c-id\sqrt{2})}{c^2+2d^2} = (\frac{ac+2bd}{c^2+2d^2}) + i(\frac{bc-ad}{c^2+2d^2})\sqrt{2} = \alpha + i\beta\sqrt{2}$*, avec* $\alpha = \frac{ac+2bd}{c^2+2d^2} \in \mathbb{Q}$ *et* $\beta = \frac{bc-ad}{c^2+2d^2} \in \mathbb{Q}$*. D'autre part, soit* $x = a + ib\sqrt{2}$*, avec* $a, b \in \mathbb{Q}$*. D'où* $a = \frac{c}{d}$ *et* $b = \frac{r}{s}$*, où* $c, r \in \mathbb{Z}$ *et* $d, s \in \mathbb{Z}^*$*. Alors* $x = \frac{cs+ird\sqrt{2}}{ds} \in Fr(A)$ *car* $cs + ird\sqrt{2} \in A$ *et* $ds \in A^*$*.*

*2)*

*a) Soit* $x = a + ib\sqrt{2} \in \mathfrak{U}(A)$. *Alors,* $\exists y = c + id\sqrt{2} \in A : xy = 1$, *d'où* $a^2 + 2b^2 = 1$ *et ainsi* $x = \pm 1$. *Comme* $\pm 1 \in \mathfrak{U}(A)$, *alors* $\mathfrak{U}(A) = \{-1, 1\}$.

*b) Soit* $x \in A : N(x)$ *est un nombre premier. Alors* $x \neq 0$ *et* $x \notin \mathfrak{U}(A)$. *Soit* $y \in A : y/x$, *alors* $\exists z \in A : x = yz$ *d'où* $N(x) = N(yz) = N(y)N(z)$ $(N(yz) = yz.\overline{yz} = y\overline{y}z\overline{z} = N(y)N(z))$. *Puisque* $N(x)$ *est un nombre premier et* $N(y)/N(x)$ *dans* $\mathbb{N}$, *alors* $N(y) = 1$ *ou* $N(y) = N(x)$. *Or, si* $N(y) = 1$, $y \in \mathfrak{U}(A)$ *et si* $N(y) = N(x)$, $N(z) = 1$, *d'où* $z \in \mathfrak{U}(A)$ *et par suite,* $x$ *et* $y$ *sont associés. Ainsi,* $x$ *est irréductible dans* $A$.

*c) Posons* $x = 1 + i\sqrt{2}$. *Puisque* $N(x) = 3$ *est un nombre premier,* $x$ *est irréductible dans* $A$. *Comme* $A$ *est principal,* $x$ *est un élément premier de* $A$.

*3)*

*a)* $A$ *est principal et* $P$ *est primitif non constant. Posons* $p = 1 + i\sqrt{2}$. *D'après 2)c),* $p$ *est premier dans* $A$. *On a* $p/3$ $(3 = (1 + i\sqrt{2})(1 - i\sqrt{2}))$, $p/9 = 3.3$, $p \nmid 1$. *Aussi* $p^2 \nmid 3$, *sinon* $p/1 - i\sqrt{2}$, *ce qui est faux car* $1 - i\sqrt{2}$ *est irréductible* $(N(1 - i\sqrt{2}) = 3$ *est un nombre premier) et* $p$ *n'est ni inversible ni associé à* $1 - i\sqrt{2}$.

*Ainsi, en utlisant le critère d'Eisenstein,* $P(X)$ *est irréductible dans* $A[X]$.

*b)* $A$ *est principal,* $P$ *est non constant, irréductible dans* $A[X]$, *alors* $P$ *est irréductible dans* $(Fr(A))[X] = (\mathbb{Q}[i\sqrt{2}])[X]$.

***Exercice 6.10***

***I)*** *Pour* $n = 2$ *: on a* $m_1 = p_1^{\beta_1}...p_r^{\beta_r}$, $m_2 = p_1^{\lambda_1}...p_r^{\lambda_r}$ $(0 \leq \beta_i, \lambda_i)$ *et* $\forall j = 1, ..., r$, $\alpha_j = \sup(\beta_j, \lambda_j)$. *Soit* $i \in \{1, ..., r\}$, *on a* $\alpha_i = \sup(\beta_i, \lambda_i)$, *alors* $p_i^{\alpha_i}/m_1$ *(si* $\alpha_i = \beta_i$*) ou* $p_i^{\alpha_i}/m_2$ *(si* $\alpha_i = \lambda_i$*).*

*Supposons que c'est vrai pour* $n - 1$.

*Pour* $n$ *: Soit* $i \in \{1, ..., r\}$. *Puisque* $ppcm(m_1, ..., m_n) = ppcm(ppcm(m_1, , ..., m_{n-1}), m_n)$ *et d'après le cas* $n = 2$, $p_i^{\alpha_i}/m_n$ *ou* $p_i^{\alpha_i}/m' = ppcm(m_1, , ..., m_{n-1})$.

*Si* $p_i^{\alpha_i}/m' = ppcm(m_1, , ..., m_{n-1})$, *alors* $m' = ppcm(m_1, , ..., m_{n-1}) = p_i^{\mu_i}.q_1^{\upsilon_1}...q_s^{\upsilon_s}$ *est la décomposition de* $m'$ *en produit de nombres premiers distincts, avec* $\alpha_i \leq \mu_i$. *D'après l'hypothèse de récurrence,* $\exists m_j \in \{m_1, , ..., m_{n-1}\}$ *tel que* $p_i^{\mu_i}/m_j$ *et donc* $\exists m_j \in \{m_1, , ..., m_{n-1}\}$ *tel que* $p_i^{\alpha_i}/m_j$ *car* $\alpha_i \leq \mu_i$.

***II)***

*1)*

*a) Posons* $\circ(a^{\frac{m}{d}}) = s$. *On a* $(a^{\frac{m}{d}})^d = a^m = e$ *d'où* $s/d$. *D'autre part,* $(a^{\frac{m}{d}})^s = a^{\frac{ms}{d}} = e$, *alors* $m/\frac{ms}{d}$ *et donc* $d/s$.

*b) Soit* $x \in \langle a \rangle \cap \langle b \rangle$, *alors* $\circ(x)/m_1$ *et* $\circ(x)/m_2$ *et donc* $\circ(x) = 1$ *car* $m_1 \wedge m_2 = 1$.

*Posons* $\circ(ab) = t$. *On a* $(ab)^{m_1m_2} = (a^{m_1})^{m_2}.(b^{m_2})^{m_1}$ *car* $G$ *est abélien. D'où* $(ab)^{m_1m_2} = e.e = e$ *et donc* $t/m_1m_2$. *D'autre part, puisque* $(ab)^t = e$ *et* $G$ *est abélien,* $a^t = b^{-t} \in \langle a \rangle \cap \langle b \rangle = \{e\}$, *alors* $m_1/t$ *et* $m_2/t$ *et donc* $m_1m_2/t$ *car* $m_1 \wedge m_2 = 1$.

*2)*

*a) On a* $m = ppcm(\circ(x), x \in G) > 1$ *car* $n \geq 2$. *Soit* $m = p_1^{\alpha_1}...p_r^{\alpha_r}$, $\alpha_1 \geq 1, ..., \alpha_r \geq 1$ ***(*)****, la décomposition de* $m$ *en produit de nombres premiers distincts.*

*Puisque* $G$ *est fini d'ordre* $n \geq 2$, *l'ensemble* $\{\circ(x)/\ x \in G\}$ *est fini de cardinal* $\geq 2$. *Alors, d'après I), pour tout* $i \in \{1, ..., r\}$, *il existe* $a_i \in G$ *tel que* $p_i^{\alpha_i}/\circ(a_i)$.

*b) Posons* $\circ(a_i) = m_i$, $d_i = p_i^{\alpha_i}$. *Comme* $d_i/m_i$, *on a, d'après II) 1)a),* $\circ(b_i = a_i^{\frac{m_i}{d_i}}) = d_i = p_i^{\alpha_i}$.

*c) Pour* $r = 2$ *: On a* $\circ(b_1) = p_1^{\alpha_1}$ *et* $\circ(b_2) = p_2^{\alpha_2}$. *Comme* $p_1 \neq p_2$, $p_1^{\alpha_1} \wedge p_2^{\alpha_2} = 1$ *et d'après II)1)b),* $\circ(b_1.b_2) = p_1^{\alpha_1}.p_2^{\alpha_2}$.

*Supposons que c'est vrai pour* $r-1$ *et montrons que c'est vrai pour* $r$ *: posons* $c = b_1...b_{r-1}$*. Alors, d'après l'hypothèse de récurrence,* $\circ(c) = p_1^{\alpha_1}...p_{r-1}^{\alpha_{r-1}}$*. Puisque* $\forall i = 1, ..., r-1,\ p_i \neq p_r$ *, on a* $\forall i = 1, ..., r-1,\ p_i^{\alpha_i} \wedge p_r^{\alpha_r} = 1$*, d'où* $\prod_{i=1}^{r-1} p_i^{\alpha_i} \wedge p_r^{\alpha_r} = 1$*, i.e.,* $\circ(c) \wedge b_r = 1$ *et ainsi, d'après II)1)b),* $\circ(b) = o(cb_r) = o(c).o(b_r) = \prod_{i=1}^{r-1} p_i^{\alpha_i}.p_r^{\alpha_r} = m$*.*

*On a* $m/n$ *car* $\circ(b)/|G|$*.*

*3) Application : D'après II)2)c) et puisque* $(K^*, .)$ *est un groupe abélien fini d'ordre* $q-1 \geq 2$*, il existe un élément* $b$ *de* $K^*$ *tel que* $\circ(b) = m = ppcm(\circ(x)/x \in K^*)$*.*

*a) On a* $\circ(b) = m/|K^*| = q-1$*, d'où* $m \leq q-1$*.*

*b) Soit* $a \in K^*$*. Alors* $\circ(a)/m = ppcm(\circ(x)/x \in K^*)$ *et donc* $a^m = 1$*.*

*c) Le polynôme* $X^m - 1 \in K[X]$ *possède au plus* $m$ *racines car* $K$ *est un corps. D'autre part, d'après 3)b),* $X^m - 1$ *possède* $q-1$ *racines distinctes, ainsi* $q - 1 \leq m$ *et* $m = q-1$*. Comme* $b$ *est un élément de* $K^*$ *d'ordre* $m = q-1 = |K^*|$*,* $K^* = < b >$*.*

## 6.4 Rattrapage (2007-2008)

**Exercice 6.11** *Soient* $G$ *un groupe abélien fini d'ordre* $n$*, noté multiplicativement,* $a$ *un élément de* $G$ *et* $H$ *un sous-groupe propre de* $G$ *tel que* $a \notin H$*. On considère l'ensemble* $N = \{t \in \mathbb{N}^*/\ a^t \in H\}$*.*

*1) Montrer que* $N$ *possède un plus petit élément. On pose* $m = inf\ N$*.*

*2) Montrer que si* $s \in N$*, alors* $m/s$*.*

*3) Montrer que l'ordre de* $\overline{a}$*, considéré comme élément du groupe* $G/H$*, est égal à* $m$*.*

*4) On considère l'ensemble* $K = \{x \in G/\ \exists j \in \mathbb{Z}, \exists h \in H : x = a^j h\} = < a > .H$*.*

*a) Montrer que* $K$ *est un sous-groupe de* $G$*, le plus petit (au sens de l'inclusion) contenant* $H$ *et* $a$*.*

*b) Vérifier que* $K/H = < \overline{a} >$ *.*

*c) En déduire que* $|K| = m|H|$*.*

*5) Application : On pose* $G = \mathbb{Z}/24\mathbb{Z}$*,* $H = 6\mathbb{Z}/24\mathbb{Z}$ *et* $a = \overline{4} \in G$*.*

*a)*

*i) Dire pourquoi* $H$ *est un sous-groupe propre de* $G$ *et vérifier que* $|H| = 4$*.*

*ii) Vérifier que* $a \notin H$ *et que* $m = 3$*.*

*b) En déduire que* $K = 2\mathbb{Z}/24\mathbb{Z}$*.*

**Exercice 6.12** *Soit* $P(X) = \frac{2}{3}X^3 + \frac{1}{2}X - \frac{1}{6} \in \mathbb{Q}[X]$ *et* $Q(X) = 4X^3 + 3X - 1 \in \mathbb{Z}[X]$*.*

*1) Montrer que* $Q(X)$ *est irréductible dans* $\mathbb{Z}[X]$ *et qu'ainsi* $P(X)$ *est irréductible dans* $\mathbb{Q}[X]$*.*

*2)*

*a) En déduire que* $K = \mathbb{Q}[X]/(P(X))$ *est un corps.*

*b) On pose* $\alpha = \bar{X} \in K$*. Dire pourquoi* $\alpha$ *est inversible dans* $K$ *et calculer son inverse.*

**Exercice 6.13**

***I)*** *Soient* $k \in 2\mathbb{Z}, k \neq 0$ *et* $N = \{s \in \mathbb{N}^*/\ 2^s$ *divise* $k\}$*.*

*1) Montrer que* $N$ *possède un plus grand élément. On note* $u = \sup N$*.*

*2) En déduire que* $k = 2^u t$*, où* $t$ *est un entier impair.*

***II)*** *On considère l'ensemble* $A_2 = \{\frac{a}{b} \in \mathbb{Q}/\ a \in \mathbb{Z},\ b \in \mathbb{N}^*$ *et* $b$ *est impair*$\}$.

*1)*

*a) Vérifier que* $A_2$ *est un anneau intègre.*

*b) Vérifier que* $\mathfrak{U}(A_2) = \{\frac{a}{b} \in A_2\ /a \in \mathbb{Z}, b \in \mathbb{N}^*,\ a$ *et* $b$ *impairs*$\}$. $A_2$ *est-il un corps ?*

*2)*

*a) Montrer que* $2$ *est irréductible dans* $A_2$.

*b) Dire pourquoi si* $u > 1$, *alors* $2^u$ *n'est pas irréductible dans* $A_2$.

*c) Soit* $x = \frac{a}{b}$ *un élément irréductible de* $A_2$ *(*$a \in \mathbb{Z},\ b \in \mathbb{N}^*$ *et* $b$ *est impair).*

*i) Dire pourquoi il existe* $k \in \mathbb{Z}^* : x = 2.\frac{k}{b}$.

*ii) Montrer que* $x \sim 2$ *dans* $A_2$ *(on suppose que* $k$ *est pair et on utilise I)2) et II) 2)b)).*

*3) On considère* $\varphi : A_2 \longrightarrow \mathbb{Z}/2\mathbb{Z},\ \frac{a}{b} \longmapsto \overline{a}$.

*a) Vérifier que* $\varphi$ *est une application bien définie et que* $\varphi$ *est un homomorphisme d'anneaux surjectif.*

*b) Montrer que* $A_2/(2) \simeq \mathbb{Z}/2\mathbb{Z}$.

**Solution**

***Exercice 6.11***

*1) On a* $N \neq \emptyset$, *car* $n \in N$, *et* $N \subset \mathbb{N}$, *alors* $N$ *possède un plus petit élément qu'on note* $m = inf N$.

*2) On effectue la division euclidienne de* $s$ *par* $m$, *alors* $\exists (q, r) \in \mathbb{N} : s = mq + r$, *avec* $0 \leq r < m$. *D'où* $a^s = (a^m)^q.a^r$ *et donc* $a^r \in H$ *car* $a^s \in H$ *et* $a^m \in H$. *Vu que* $m$ *est le plus petit entier* $> 0$ *tel que* $a^m \in H$ *et que* $0 \leq r < m$, *alors* $r = 0$.

*3) On a* $a^m \in H$, *d'où* $\overline{a}^m = \overline{e}$ *et ainsi* $\circ(\overline{a})/m$. *D'autre part,* $\overline{a}^{\circ(\overline{a})} = \overline{e}$, *d'où* $a^{\circ(\overline{a})} \in H$ *et donc* $m/\circ(\overline{a})$. *Ainsi* $\circ(\overline{a}) = m$.

*4)*

*a) Il est évident que* $K$ *est un sous-groupe de* $G$, *que* $a \in K$, *et que* $H \subset K$. *Soit* $K'$ *un sous-groupe de* $G$ *contenant* $a$ *et* $H$. *Puisque* $\forall j \in \mathbb{Z},\ a^j \in K',\ H \subset K'$, *on a* $a^j h \in K',\ \forall j \in \mathbb{Z},\ \forall h \in H$, *i.e.,* $K \subset K'$.

*b) Soit* $a^j h \in K$, *alors* $\overline{a^j h} = \overline{a^j}.\overline{h} = \overline{a^j} \in <\overline{a}>$ *car* $h \in H$. *D'autre part, soit* $\overline{a^j} \in <\overline{a}>$, *alors* $\overline{a^j} = \overline{a^j.e} \in K/H$ *car* $a^j.e \in K$.

*c)* $K$ *est un sous-groupe fini de* $G$ *et* $K/H$ *est un sous-groupe de* $G/H$, *d'où* $|K/H| = \frac{|K|}{|H|} = \circ(\overline{a}) = m$ *et ainsi* $|K| = m|H|$.

*5) Application :*

*a)*

*i) On a* $6\mathbb{Z}$ *est sous-groupe de* $\mathbb{Z}$ *et puisque* $6/24$, $24\mathbb{Z} \subset 6\mathbb{Z}$, *alors* $6\mathbb{Z}/24\mathbb{Z}$ *est un sous groupe de* $\mathbb{Z}/24\mathbb{Z}$. *On a aussi* $6\mathbb{Z}/24\mathbb{Z} \neq \mathbb{Z}/24\mathbb{Z}$ *car* $6$ *et* $24$ *ne sont pas premiers entre eux. Comme* $(\mathbb{Z}/24\mathbb{Z})/(6\mathbb{Z}/24\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z}$, *on a* $|H| = \frac{24}{6} = 4$.

*ii) On a* $\overline{4} \notin (6\mathbb{Z}/24\mathbb{Z})$, *sinon* $\overline{4} = \overline{6k}$, *alors* $24/4 - 6k$ *et par suite* $6/4 - 6k$ *et ainsi* $6/4$, *ce qui est faux.*

*On a aussi* $2.\overline{4} \notin (6\mathbb{Z}/24\mathbb{Z})$. *Cependant,* $3.\overline{4} = \overline{12} = \overline{6.2} \in H$, *ainsi* $m = 3$.

*b) On a* $|K| = m|H| = 3.4 = 12$. *Puisque* $K$ *est un sous-groupe de* $\mathbb{Z}/24\mathbb{Z}$, *alors* $K = t\mathbb{Z}/24\mathbb{Z}$, *avec* $t/24$. *D'autre part, d'après le 3ème théorème d'isomorphisme,* $(\mathbb{Z}/24\mathbb{Z})/(t\mathbb{Z}/24\mathbb{Z}) \simeq \mathbb{Z}/t\mathbb{Z}$, *alors* $\frac{|G|}{|K|} = t$ *et donc* $t = \frac{24}{12} = 2$, *i.e.,* $K = 2\mathbb{Z}/24\mathbb{Z}$.

***Exercice 6.12***

*1) On a $\mathbb{Z}$ est un anneau principal, $Q(X)$ est primitif et non constant, $p = 5$ est premier dans $\mathbb{Z}$ et $p = 5 \nmid 4$. En utilisant la réduction modulo $p = 5$, on a $\varphi_5(Q) = \overline{4}X^3 + \overline{3}X - \overline{1} \in (\mathbb{Z}/5\mathbb{Z})[X]$ est un polynôme de degré 3, $\varphi_5(Q)$ n'a pas de racine dans $\mathbb{Z}/5\mathbb{Z}$ ($\varphi_5(Q)(\overline{0}) = \overline{4}, \varphi_5(Q)(\overline{1}) = \overline{1}, \varphi_5(Q)(\overline{2}) = \overline{3}, \varphi_5(Q)(\overline{3}) = \overline{3}, \varphi_5(Q)(\overline{4}) = \overline{2}$), d'où $\varphi_5(Q)$ est irréductible dans $\mathbb{Z}/\mathbb{Z}Z[X]$ et par suite $Q(X)$ est irréductible dans $\mathbb{Z}[X]$.*

*Comme $\mathbb{Z}$ est principal, $\mathbb{Q} = Fr(\mathbb{Z})$ et $Q(X)$ est un polynôme non constant, irréductible dans $\mathbb{Z}[X]$, alors $Q(X)$ est irréductible dans $\mathbb{Q}[X]$.*

*D'autre part, puisque $Q(X) = 6P(X)$, alors $P(X)$ et $Q(X)$ sont associés dans $\mathbb{Q}[X]$ et ainsi $P(X)$ est irrédutible dans $\mathbb{Q}[X]$.*

*2)*

*a) Comme $\mathbb{Q}$ est un corps et $P(X)$ est irréductible dans $\mathbb{Q}[X]$, alors $(P(X))$ est un idéal maximal de l'anneau principal $\mathbb{Q}[X]$ et par suite $K = \mathbb{Q}[X]/(P(X))$ est un corps.*

*b) On $\alpha = \overline{X} \neq \overline{0}$ dans $K$ car $P(X) \nmid X$ dans $\mathbb{Q}[X]$ et donc $\alpha$ est inversible dans $K$. Pour calculer $\alpha^{-1}$, il suffit de remarquer que $\overline{P(X)} = \overline{\frac{2}{3}X^3 + \frac{1}{2}X - \frac{1}{6}} = \overline{0}$ dans $K$ et ainsi $\alpha^{-1} = \overline{4X^2 + 3}$.*

***Exercice 6.13***

***I)***

*1) On $N \subset \mathbb{N}$, $N \neq \emptyset$ car $1 \in N$, $N$ est majorée car $\forall s \in N, s \leq \frac{|k|}{\log 2}$ et par suite $N$ possède un plus grand élément. On note $u = supN$.*

*2) On a $u \in N$, alors $k = 2^u.t$, où $t \in \mathbb{Z}$. Ainsi, $t$ est impair, sinon $2^{u+1}/k$, ce qui contredit le fait que $u = supN$.*

***II)***

*1)*

*a) Il suffit de vérifier que $A_2$ est un sous-anneau de $\mathbb{Q}$.*

*b) Soit $\frac{a}{b} \in \mathfrak{U}(A_2)$, où $a \in \mathbb{Z}, b \in \mathbb{N}^*$ et $b$ impair, alors $\exists \frac{c}{d} \in A_2$, où $c \in \mathbb{Z}, d \in \mathbb{N}^*$ et $d$ impair: $\frac{a}{b}.\frac{c}{d} = 1$, d'où $ac = bd$ est impair et donc $a$ est impair. D'autre part, si $\frac{a}{b} \in A_2$, $a \in \mathbb{Z}, b \in \mathbb{N}^*$ et $a, b$ impairs, alors $\frac{a}{b}.\frac{b}{|a|} = \pm 1$ et ainsi $\mathfrak{U}(A_2) = \{\frac{a}{b} \in A_2 \; /a \in \mathbb{Z}, b \in \mathbb{N}^*$, $a$ et $b$ impairs$\}$. Puisque $\mathfrak{U}(A_2) \neq A_2 - \{0\}$ (par exemple $2 \notin \mathfrak{U}(A_2)$), $A_2$ n'est pas un corps.*

*2)*

*a) On a $2 \notin \mathfrak{U}(A_2)$. Soit $\frac{a}{b} \in A_2$, où $a \in \mathbb{Z}, b \in \mathbb{N}^*$, $b$ impair, tel que $\frac{a}{b}/2$, alors $\exists \frac{c}{d} \in A_2$, où $c \in \mathbb{Z}, d \in \mathbb{N}^*$ et $d$ impair : $\frac{a}{b}.\frac{c}{d} = 2$, d'où $2bd = ac$ ainsi $2/a$ ou $2/c$. Supposons que $2/a$, alors $2bd = 2kc$ ($a = 2k$), donc $bd = kc$ d'où $c$ est impair et par suite $\frac{c}{d} \in \mathfrak{U}(A_2)$, alors $\frac{a}{b} \sim 2$. De même, si $2/c$, alors $a$ est impair et donc $\frac{a}{b} \in \mathfrak{U}(A_2)$. Ainsi, 2 est irréductible dans $A_2$.*

*b) Si $u > 1$, alors $2^u$ n'est pas irréductible dans $A_2$ car $2/2^u$ et 2 n'est ni inversible ni associé à $2^u$ ($2^{u-1} \notin \mathfrak{U}(A_2)$ car $u - 1 \geq 1$).*

*c)*

*i) Soit $x = \frac{a}{b}$ un élément irréductible de $A_2$, où $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et $b$ est impair, alors $a \in 2\mathbb{Z}$ et $a$ est non nul car $x$ est non inversible et non nul, d'où $\exists k \in \mathbb{Z}^* : x = 2.\frac{k}{b}$.*

*ii) On suppose que l'entier non nul $k$ est pair, alors, d'après I)2), $k = 2^u.t$, où $u \geq 1$, $t \in \mathbb{Z}$ est impair. Donc $x = 2^{u+1}.\frac{t}{b}$ et ainsi $x \sim 2^{u+1}$ car $\frac{t}{b} \in \mathfrak{U}(A_2)$. Or, d'après II)2)b), $2^{u+1}$ n'est pas irréductible, contradiction. Alors $k$ est impair et donc $x \sim 2$ car $\frac{k}{b} \in \mathfrak{U}(A_2)$.*

*3) $\varphi$ est bien définie. En effet, soient $\frac{a}{b} = \frac{c}{d} \in A_2$, où $a, c \in \mathbb{Z}, b, d \in \mathbb{N}^*$ et $b, d$ impairs. On a $ad = bc$, d'où $\overline{a}.\overline{d} = \overline{b}.\overline{c}$ dans $\mathbb{Z}/2\mathbb{Z}$, et ainsi $\overline{a} = \overline{c}$ (car $b$ et $d$ sont impairs).*

*Soient $\frac{a}{b}, \frac{c}{d} \in A_2$ ($a, c \in \mathbb{Z}, b, d \in \mathbb{N}^*$ et $b, d$ impairs). On a $\varphi(\frac{a}{b} + \frac{c}{d}) = \varphi(\frac{ad+bc}{bd}) = \overline{ad + bc} = \overline{a} + \overline{c}$ car $\overline{b} = \overline{d} = \overline{1}$, d'où $\varphi(\frac{a}{b} + \frac{c}{d}) = \varphi(\frac{a}{b}) + \varphi(\frac{c}{d})$. On a aussi $\varphi(\frac{a}{b}.\frac{c}{d}) = \varphi(\frac{a}{b}).\varphi(\frac{c}{d})$ et $\varphi(1) = \overline{1}$,*

*ainsi* $\varphi$ *est un homomorphisme d'anneaux.*

$\varphi$ *est surjectif car* $\forall \overline{a} \in \mathbb{Z}/2\mathbb{Z}, \exists x = \frac{a}{1} \in A_2 : \varphi(x) = \overline{a}$.

*b) Montrons que* $ker\varphi = (2)$. *On* $2 \in ker\varphi$, *d'où* $(2) \subset \ker\varphi$. *D'autre part, soit* $\frac{a}{b} \ker\varphi$, *avec* $a \in \mathbb{Z}, b \in \mathbb{N}^*$ *et* $b$ *impair, alors* $a \in 2\mathbb{Z}$, *d'où* $\exists k \in \mathbb{Z} : \frac{a}{b} = 2.\frac{k}{b}$, *ainsi* $\frac{a}{b} \in (2)$.

*D'après le 1*$^{er}$ *théorème d'isomorphisme, on a* $A_2/(2) \simeq \mathbb{Z}/2\mathbb{Z}$.